DIGITAL CURATION OF RECORDS IN THE CLOUD TO SUPPORT E-GOVERNMENT SERVICES IN SOUTH AFRICA

BADIMUNI AMOS SHIBAMBU

Student Number 60873329

Submitted in accordance with requirements for the degree of

DOCTOR OF LITERATURE AND PHILOSOPHY

in the subject

INFORMATION SCIENCE

at the

UNIVERSITY OF SOUTH AFRICA

Supervisor: Prof M Ngoepe

November 2019

SUMMARY

Many scholars lament of poor infrastructure to manage and preserve digital records within the public sector in South Africa to support electronic government (e-government). For example, in South Africa, the national archives' repository and its subsidiary provincial archives do not have infrastructure to ingest digital records into archival custody. As a result, digital records are left to the creating agencies to manage and preserve. The problem is compounded by the fact that very few public sector organisations in South Africa have procured systems to manage digital records. Therefore, a question is how are digital records managed and stored in these organisations to support e-government? Do public organisations entrust their records to the cloud as an alternative storage given the fact that both physical and virtual storages are a problem? If they do, how do they ensure accessibility, governance, security and long-term preservation of records in the cloud? Utilising the Digital Curation Centre (DCC) Lifecycle Model as a guiding framework, this qualitative study sought to explore digital curation of records in the cloud to support e-government services in South Africa with the view to propose a framework that would guide the public sector to migrate records to the cloud storage. Semi-structured interviews were employed to collect data from the purposively selected Chief Information Officers in the national government departments that have implemented some of the electronic services such as the Department of Arts and Culture, Department of Home Affairs, Department of Higher Education and Training and the Department of Basic Education.

Furthermore, the National Archives and Records Services of South Africa was also chosen as it is charged with the statutory regulatory role of records management in governmental bodies. So is the State Information Technology Agency (SITA), a public sector ICT company established in 1999 to consolidate and coordinate the state's information technology resources in order to achieve cost savings through scale, increase delivery capabilities and enhance interoperability. Interview data were augmented through document analysis of legislation and policies pertaining to data storage. Data were analysed thematically and interpreted in accordance with the objectives of the study. The key finding suggests that although public servants informally and unconsciously put some records in the clouds, government departments

in South Africa are sceptical to entrust their records to the cloud due to a number of reasons, such as lack of policy and legislative framework, lack of trust to the cloud storage, jurisdiction, legal implications, privacy, ownership and security risks. This study recommends that given the evolution of technology, the government should regulate cloud storage through policy and legislative promulgation, as well as developing a government-owned cloud managed through SITA in order for all government departments to use it. This study suggests a framework to migrate paper-based records to cloud storage that is controlled by the government.

Key words: digital curation, cloud storage, electronic government, digital records, digital disposal, digital preservation, archives, legislation, cloud application, cloud services, records management, South Africa

ACKNOWLEDGMENTS

Embarking on a journey to conduct a doctoral study is a torturous exercise. It is capable of isolating one from significant aspects of life such as running, relatives, friends, work, family members and many more activities. It confines one to the fountain of various books. I feel incredibly humbled and privileged to express my gratitude to the people that have supported me to get to this point in my career. Pursuing a PhD has always been a wish, but courage was never there. However, different people irrespective of their level of education made it a point that I receive courage. During this course, the regular people I associated with, were the academic promoter, academic friends and special friends who have endeared themselves to my heart and work. Their key phrase was "you are almost there" as if I was participating in a Comrades Ultramarathon from Durban to Pietermaritzburg, a torturous 87km. Without the cheerleaders, the stage of bailing out of this solitary confinement was looming across the horizon. I am even finding it difficult to mention their names. However, this would never have happened without the involvement of Professor Mpho Ngoepe. His academic inspiration displayed itself when I was doing my Master's in Business Information Systems at the Tshwane University of Technology. He said "finish your Master's Degree so that you can enrol for PhD with UNISA to be able to define your tomorrow. At UNISA, the inputs you make is the output you get". These words kept me going. On the other hand, Dr Jan Maluleka was always ready with words of encouragement and better ways to find answers for my thesis while we were jogging the hills of the Union Buildings and Pretoria East in preparation of the races. In reality and given the immense role you played, it is not possible to mention every individual who contributed to this thesis directly or indirectly. However, my sincere appreciation goes to the following people:

- My parents Samson and Elisah Shibambu. Despite their elementary education, they always encouraged me to never stop studying. Indeed, I heeded their calls.
- The participants who accommodated me in their busy schedules for the interviews. The project would not have been completed without your cooperation.
- The University of South Africa's Research Directorate for funding my study.
- Finally, thanks to every helping hand that contributed to the success of this thesis, Xikwembu xi mi katekisa.

DEDICATION

This thesis is dedicated to the all government departments that are looking forward to making information accessible without the hindrance of time and place. To them I say, cloud is the way to go.

To my parents, kids and Shibambu families, friends, brothers and sisters, here is another achievement.

DECLARATION

Name: Badimuni Amos Shibambu

Student number: 60873329

Degree: Doctor of Philosophy in Information Science

Digital curation of records in the cloud to support e-government services in South Africa

I declare that the above dissertation is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

I further declare that I submitted the dissertation to originality checking software and that it falls within the accepted requirements for originality.

I further declare that I have not previously submitted this work, or part of it, for examination at Unisa for another qualification or at any other higher education institution.

SIGNATURE

16 December 2019

DATE

TABLE OF CONTENTS

PAGES

LIST OF ABBREVIATIONS

API	Application program interface
CEO	Chief Executive Officers
CIO	Chief Information Officers
CSP	Cloud service providers
DAC	Department of Arts and Culture
DBE	Department of Basic Education
DCC	Data Curation Centre
DHET	Department of Higher Education and Training
DOD	Department of Defence
DST	Department of Science and Technology
DTPS	Department of Telecommunications and Postal Services
E-banking	Electronic banking
E-commerce	Electronic commerce
ECT	Electronic communications and Transactions Act
E-government	Electronic government
G2C	Government and citizens
G2G	Inter-agency relationship
GITC	general information technology controls ()
IaaS	Infrastructure as a service
ICA	International Council on Archives
ICT	Information and communications technology
IODSA	Institute of Directors Southern Africa
IRMT	International Records Management Trust
ISA	International Standard Authority
ISAAR	International Standard Archival Authority Record for Corporate Bodies, Persons and Families
ISAI	Standard of Archival Institutions
ISD	International Standard for Archival Description
ISDIAH	International Standard for Describing Institutions with Archival Holdings
ISO	International organisation for standardisation
IT	Information technology

LAN	Local area network
MIT	Massachusetts Institute of Technology
NARA	National Archives and Records Administration
NARSA	National Archives of South Africa Act
NARSSA	National Archives and Records Services
NAS	Network attached storage
PaaS	Platform as a service
PAIA	Access to Information Act
POPI	Protection of Personal Information Act,
SaaS	Software as a server
SAN	Storage area networks
SITA	State Information Technology Agency
UNISA	University of South Africa
VPN-C	Virtual private network connection
WWW	World Wide Web

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

MOVING AWAY FROM TRADITIONAL RECORD-KEEPING TO DIGITAL ENVIRONMENT

1.1 Introduction and background to the study

The significance of cloud storage to electronic government (e-government) is well documented and it improves ways of providing services to the citizens of a country. For example, Paquette, Jaeger and Wilson (2010:247) indicate that former president of the United States of America, Barak Obama, propounds that cloud computing is capable of opening up the government to its citizens. Hu, Wang, Pan and Shi (2011) concur that the contribution of cloud storage to e-government services has the potential to merge distance and space, as well as reduce time, which makes the transactions of public service more effective. Indeed, it contributes positively in both public and private sectors where paper-based records have been converted to digital records in order to achieve longer lasting records that are accessible online. Following its impressive work, Shen, Yang and Keskin (2012) retrospectively trace the idea of cloud computing to 1961 when John McCarthy predicted while publicly giving a speech to celebrate the Massachusetts Institute of Technology's (MIT) centennial that computation may someday be organised as a public utility. Kriesberg (2017) opines that the increasingly widespread adoption of computers during the second half of the 20th century changed ways in which society creates and interacts with information, playing a disruptive role and forcing organisations to adapt or be left behind. Just like electricity and the telephone, subscribers need to pay for the capacity of the usage of the space they acquired from the cloud service providers (CSP). The situation leads to more storage for digital records in the cloud.

Cunningham (2008) mentions that archival programmes worldwide spend every cent they could spare researching digital preservation. The cloud storage has become part of every Chief Executive Officer's (CEO) agenda as it gains more popularity where Gartner ranked it among the top ten strategic technologies for 2011 (Shen et al 2012). In the wake of such evolution, the CEOs routinely talk about strategic value of information technology (IT) with a way of gaining competitive advantage and digitalisation of business models. As a result, Chief Information Offers' (CIO) positions are created and appointed to provide fresh ideas on how to leverage IT investment for the purpose of implementing cloud storage in their organisations. This is

influenced by the fact that the major goal of cloud computing is to reduce the cost of IT services while increasing processing throughput, reliability, availability and flexibility of business operations (Oredo, Njihia & Iraki 2017). According to Trope (2014), a study conducted in South Africa indicates that the information and communications technology (ICT) sector is leading in cloud computing by 54% while the financial sector is at 33%. Bettacchi, Re and Polzonetti (2017:79) are in agreement that cloud storage in all its aspects "covers a wide range of strategic sectors, both public and private", allowing the consumers to realise shared infrastructure that significantly facilitates design, application and management of information storage. Adoption of cloud storage has the potential to retain records in good quality.

Wahsh and Dhillon (2015) espouse that in the context of public administration, storing records in the cloud seems to be the most cost-effective means of delivering e-government services towards ensuring efficiency, effectiveness, transparency, interoperability, cooperation, sharing and security. All that drive the transition to a public service of the 21st century; paying attention on the needs of citizens. Bouaziz (2008:12) also mentions that the popular roles of e-government services are to allow collaboration of the government and its citizens (G2C) and to enable inter-agency relationship (G2G). However, that is achievable in the presence of cloud computing and digital preservation, which enable retrieval of records in various places at the same time. Carter and Bélanger (2005:5) observe that one of the primary functions of e-government is to add the expediency and accessibility of government services to citizens and to promote cost-effective government. Its success is solely reliant on a platform of cloud storage. In all organisations, data ostensibly has been a strategic tool that is needed to make informed decisions and to perform activities successfully.

Hu et al (2011) postulate that storing records in the cloud improves transparency and provision of government services in the government departments as has been seen in countries like Canada, United States of America, United Kingdom and China, to mention but a few. The same cannot be said about the states in the global periphery like the Republic of South Africa. In situations where cloud storage is used, those in need of information would not visit a physical location, because the required records and information would be accessed virtually from the cloud storage. In addition, government departments would securely share digitised archived records with others, contrary to the current storage arrangement where people need to physically visit the record-keeping areas. Van Jaarsveldt and Wessels (2015:2) posit that governments worldwide are working hard to provide advanced IT-enabled public services to

their citizens. The National e-Strategy as contained in the Electronic Communications and Transactions Act (ECTA) No. 25 of 2002 mentions that e-government dates back to 1995 when the White Paper on the transformation of public service was released. However the pace has been very slow. This can be noticed in the islands of e-government initiatives in the country where others have been highly successful and are worth replicating. Given that the South African government envisions the offerings of government services through e-government services, and has already partially realised the vision (application of identity documents, passport online, as well as filing of tax returns), it is necessary to have digital preservation in the cloud in order to support such services (Ngoepe 2014). The author further contends that infrastructure for digital preservation does not exist.

While the findings of iResearch of 2012 indicate that cloud storage service is already technically matured, its promotion is still in its infancy and that can be ostensibly seen in the way record-keeping is handled. South African government departments have their records in their registries where they are manually accessed because they are prominently stored in the form of paper medium, audio-visual and microfilm (Ngoepe 2012). The author further points out that notwithstanding the importance of cloud storage, the challenge with the current practice in the context of the South African government, records are stored on the premises of each department's registries manned by untrained registry clerks. Only a few governmental bodies have automated their records management programme (Ngoepe 2011). Pickover and Harris (2001) maintain that traditional paper-based records are likely to be inefficiently provided with resources, manned by junior record practitioners with little status and subject to high turnover rates, and incorrectly connected, if at all, to parallel or similar electronic record management system. This statuesque as observed by Ngoepe (2014) is still prevalent. Rightly so, cloud storage is not prevalent among government departments in South Africa. For example, Kuiper, Van Dam, Reiter and Janssen (2014:1) opine that despite the potential advantages offered by cloud computing, such as cost reduction in setting up cloud storage infrastructure, increased flexibility and agility when sharing archived records, the public sector in South Africa lags behind. On the other hand, Ngoepe (2014) mentions that although public servants informally and unconsciously put some records in the cloud, government departments in South Africa are sceptical to entrust their data to the CSP due to reasons comprising the lack of trust in the cloud storage, jurisdiction, legal implications, data privacy and security risk related to the Minimum Information Security Standards (MISS). The author further argues that this leaves the government departments to face challenges like limited access to data in the

provision of improved service delivery, as well as a lack of storage space for both paper and digital records. The problem is compounded by a lack of government policy or legislation that regulates the storage and digital curation of records in the cloud.

In South Africa, the responsibility of regulating government records to support e-government falls under the auspices of the National Archives and Records Services (NARSSA), which according to Ngoepe (2014), has not designed the necessary infrastructure to manage and preserve digital records. As a result, the absence of policies that regulate the storage of records in the cloud leaves government departments to put away hard copies in an inaccessible storage with only a few authorised users to ensure that it retains its integrity and authenticity (Higgins 2011:79). This study utilised the Data Curation Centre (DCC) Lifecycle model to explore digital curation of records in the cloud to support e-government services in South Africa.

1.1.1 Brief history of record-keeping in South Africa

Ngoepe (2008:61) points out that in South African, paper-based record keeping can be traced through the history of NARSSA. According to Ngulube (2006), during that time when paper-based record keeping was prevalent, a part of South Africa was still called the Cape Colony. Cunningham (2008) and Kumar et al (2011) argue that the predecessors of archives used words like metadata to describe the documentation systems. These archivists implemented impressive regimes for carrying non-digital archives and records forward to the current archival programmes. Congruent to that, Ngoepe (2008:62) further adds that South Africa's oldest record dates back to 1651, which can only be accessed by physically visiting the Cape Archives Repository in Cape Town. IT literature reveals that paper-based record keeping was relevant considering that the computers were not ubiquitous to be used for record keeping developed during the 1970s (Yang, Zhang, Ding & Zheng 2016). Its use led to the development of cloud storage that precedes various forms of data-keeping methods by the government. The authors opine that the introduction of cloud computing allows storage and access to online services. For instance, as mentioned earlier on, the South African Department of Home Affairs has made a notable achievement by allowing citizens to apply for their identity documents and passports by using biometrics for authentication at some bank branches around the country. Instead of physically going to apply for the identity document or passport at the department, the citizens apply through its website. In this case, the process is completed without physical interaction between the department and citizens. To improve efficiency, the department has created a

public-private partnership with some banks in order to make e-government services effective. This shows how much reliance e-government service has on cloud storage. This, in line with the National E-government Strategy and Roadmap, which forms part of Electronic and Communications Transactions Act (ECTA) No. 25 of 2002 is an indication that e-government service is about transforming government to be more citizen-centred. Such service is an example of government to citizen (G2C), which involves an interaction between government and its citizens. This shows that e-government services offer an opportunity to store government records in trusted digital repositories. Sarkar and Kumar (2016:320) postulate that data storage is a prominent feature that CSP provides to its clients in order to store huge amounts of storage capacity, and to provide many services to the clients by cloud. In the same view, Kriesberg (2015) indicates that in this environment, private organisations provide the possibility of working towards the archival mission while creating digitised copies of records and placing them on popular web portals which users already access.

Marutha (2011:21) mentions that the benefits of the governments that properly manage their records are not narrowed to easy retrieval and access to records, capability to avert and track fraud and corruption, easy to follow knowledgeable problem-solving and decision-making as well as the security of the institutions against lawsuits. The author further explains that proper records management helps the organisations to preserve well-organised records in their businesses. The NARSSA (2007:1) elucidates that well-organised records management provides evidence of business in the context of cultural activity and contributes to the collective memory of the nation. This study argues that remaining dependent on the storage media, as currently practised by many South African government departments, does not promote e-government where citizens take advantage of ICT.

Ojo (2014) observes that governments make use of ICT to support e-government services, and specifically the internet in order to enhance government operations, involve citizens and deliver the government services. Nam (2012:364) contends that while ICT is considered meaningful as a functional extension, it should not be viewed as a replacement of the government the citizens are familiar with. Shim and Eom (2009:100) expound that e-government is seen to be playing a significant role in the public administration and management reform. Venkatesh, Chan and Thong (2012:116) suggest that the interaction might be in the form of obtaining information, filings, sharing data, making payments and a host of other activities via the World Wide Web (www). Such practice means that the government departments should have physical

papers digitised at their disposal and upload them to the cloud data storage so that they can be shared digitally through cloud computing. According to Arshad et al (2014), it is imperative to create conditions where the necessary information is provided to the right people, at a right time and place in an optimal form and volume. This study used the Digital Curation Centre Lifecycle model to explore the implementation of digital management in cloud storage with a view to support e-government services in South Africa. The selected constructs from the model include storage, disposal and digital preservation.

1.1.2 Overview of archiving in South Africa

The NARS came as a result of appointing an Archives Commission of the Cape Colony in 1877, and after the Union, in the employment of a Chief Archivist for the Union of South Africa in 1919 leading to the first promulgation of the initial archive Act in 1922. All of the government archiving services in the country were geographically decentralised with archives repositories being maintained in every provincial capital, under central administrative management of a head office. This is a reflection that decentralisation of data storage has been in existence for time immemorial. The decentralisation of data storage in the registry of each department in various forms of media other than digital preservation in a central storage where accessibility would be easy was never introduced.

Despite the promulgation of the NARSA Act (No. 43 of 1996) (as amended) that stipulated the basis for the transformation of the archives system and its arrangement with the requirements of the democratic South Africa, record keeping remains prominently paper based. Schedule Five of the South African Constitution of 1996 outlines for the archives other than national archives to be in a limited provincial capability. Considering that South Africa was composed of four provinces (Natal, Transvaal, Orange Free State and Cape Colony), the Public Archives Act of 1922 was promulgated in order to regulate the activities of the government archives services. This Act defined the fundamentals for an undeviating system of arrangements, description, compilation of lists, inventories and other necessary finding aids for archives and records. These fundamental were meant to be applied by all provinces in their archives.

Davies (1960) states that like South Africa's international counterparts where an avalanche of unarranged, scattered documents as well as low number of records practitioners possessing archival-keeping skills, the government archives formed closer relationships with the entire

government administration with the purpose of guarding the destiny of South Africa's archival heritage. Davies (1960) further indicates that in 1953, a new archives Act was promulgated, with a view to create the cornerstone of the Archives Commission that would approve the disposal of unimportant records, documents and other materials in any public archives repository or governmental body in the form of destruction.

1.2 Theoretical framework underpinning this study

A system of interrelated concepts that is capable to condense and put together knowledge about the social world is regarded as social theory (Neuman 2006). Miles and Huberman (1994) and Miles, Huberman & Saldana (2016) further mention that social theories have an important function in research that are a crucial supporter for the scholar. Given the number of frameworks developed for digital preservation, this study is underpinned to the Data Curation Centre (DCC) Lifecycle Model that was developed by Digital Curation Centre. Cunningham (2008) defines DCC as the maintaining and adding value to a trusted body of digital information for current and future use. It combines diverse threads of similar professional attempts spanning the whole life of digital information into a coherent whole. Considering that it can be used in various domains, digital archiving is different from digital libraries and digital museums. Cunningham (2008) observes that archiving ensures that records, which have value as authentic evidence of administration, corporate, cultural and intellectual activities, are made, kept and used. The author indicates that records provide evidential decisions and activities of the institution. In relation to the present study, Jing and Fang (2017) mention that in countries such as Britain, "data curation" is referred to as digital curation wherein data refer to scientific data. The term "curation" was originally used in the protection of cultural heritage in the West of Europe, referring to planning, selection, continuous maintenance and exhibition of collections that advance the displaying rate.

The DCC Lifecycle model is relevant to this study because it shows that the current practice of record keeping in South Africa can be digitised and migrated to the cloud storage as has been seen in countries such as the United States of America and the United Kingdom. Initially, libraries these countries used this model to digitise the study material with a purpose to reduce congestion by creating online access anywhere at any time. Furthermore, data curation, which is the theoretical framework underpinning this study, means "activities that are similar to the managing and improving of data from the minute of their creation to ensure present purposes

and obtainability for prospective rediscovery and reuse of data". As envisioned by the government of the Republic of South Africa, digital preservation is a fundamental cornerstone of e-government services. Digital preservation is a significant base for the e-government services as envisioned by the South African government. Central to the functions, this model encourages digital preservation, which enables easy access to records. For that purpose, it continuously requires updates so that data meet the demands of those who are in need of it.

As indicated in Figure 1.1, the model presents the realisation of digital curation process, which is created by the cyclic structure comprising of data, description of data, preservation plan of long-term data, sharing of data, participation of community group activity, management of data, lifecycle of data layer, conceptualisation of data, creation or receiving, appraisal and selection, transmission of data to the data centre, action of long-term preservation, storage, reuse/access, transformation, disposal, reappraisal and migration. In relation to the model, it can be interpreted that digital curation of data is a process of selectively effecting the continuous and systematic maintenance and management of dependable scientific data with reuse value from its creation in connection with scientific data lifecycle to enable reuse and addition of value to data, comprising a series of activities like scientific planning, creation of data or collection appraisal and selection, organisation and disposal, description, transformation, storage and reuse.

Halbert, Skinner and McMillan (2008:90) suggest that while the South African government departments continue to use paper-based records, this the DCC lifecycle model supports institutions that store, manage, preserve as well as dispose of digital records in order to safeguard continuous long term usage of records. Yakel (2007) reveals that digital curation actively involves information professionals in the management, including the preservation of digital records for future use. In addition, many people have been performing various aspects of digital curation of records for many years but, modern and recent events have brought with them a number of views, organisations and individuals together to pay attention very intently on digital curation. According to Yakel (2007), reports in the United States by the National Science Foundation and the American Council of Learned Societies and in the United Kingdom by Lyon of UKOLN have revealed that the aspects of digital curation, which need to be in place to ensure that digital objects can be maintained, preserved, and remain available for future use. According to Higgins (2008), in the wake of doing away with practices of paper-based records, digital curation of records has

prominently become an umbrella concept that includes elements such as digital preservation, data curation and digital assets management. The author also opines that the evolution of technology within the scientific records and documentation of heritage are increasingly created in digital format where this model plays a significant role. Geerts, Kementsietsidis and Milano (2006) also predicted that the digital revolution would enable data and information to be transmitted to all corners of the world.

In libraries, this model encourages institutions to look at the digitalisation processes holistically in terms of action and policies (Nyide 2017). Rightly so, Jing and Fang (2017) confirm that the libraries in the institutions of higher learning have started implementing scientific and technological management activities of information, for instance, searching, collection, processing, analysis, storage, transmission, sharing and long-term preservation using the DCC lifecycle model. In South Africa, various libraries such as at the University of KwaZulu-Natal have adopted this model to digitise their theses and dissertations. According to Hirwade, as cited by Nyide (2017), this model has assisted the university's library to digitally preserve theses and dissertations and these must be made accessible to everyone regardless of where they are. This indicates that digital preservation using this model of cloud storage which leads to online services, is enhanced. This practice was adopted after seeing the benefits the model reflected in the libraries of the universities in the United States of America (Nyide 2017). Higgins (2008:137) advises that taking managerial and administrative actions that promote digital curation of records throughout the lifecycle assists in keeping a close eye on the creation of data and encourages best practices through policies and standards to improve the organisation of data throughout its lifecycle. In a similar fashion, this model can be used in the records management environment to digitise the current archiving method, and migrate to cloud storage with an intention to enhance e-government services in the South African government departments.

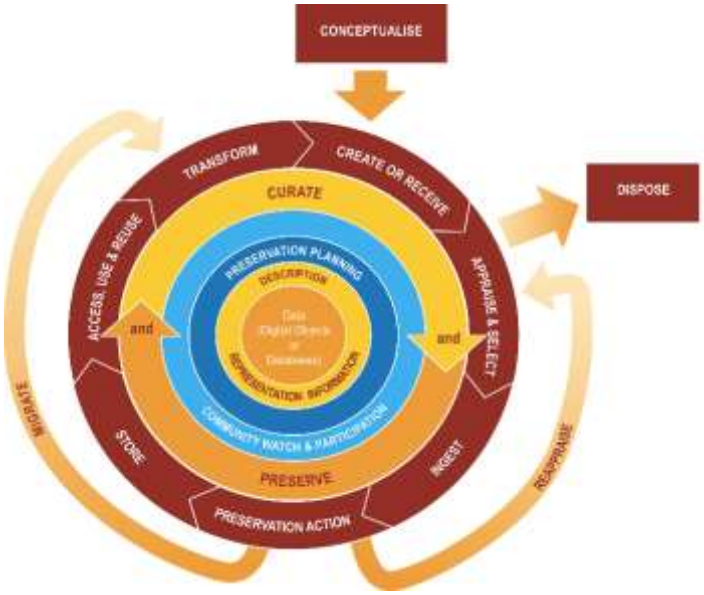

Figure 1.1 Data Curation Centre Lifecycle Model (Higgins 2008:136)

Higgins (2011) and Constantopoulos et al (2009) point out that DCC Lifecylce model, as partitioned into three categories (full lifecycle, sequential and occasional actions) was purposefully designed to facilitate the organisations and planning of curation and preservation activities within an organisation through the introduction of a series of planned actions and policies. The constructs of the model are discussed as follows:

Full lifecycle actions

Higgins (2011), Constantopoulos and Dallas (2008) and Constantopoulos et al (2009) explain that full lifecycle actions comprise a set of actions that need to be performed throughout the lifecycle of digital objects and they are as follows:

- Description and representation information: this is composed of administrative, descriptive, technical, structural and preservation metadata that are essential to define a digital object in the long term with the information necessary to understand and render the object and metadata.
- Preservation planning: this action comprises the necessary administrative and management plans for the actions of the lifecycle model. It cautions to plan for preservation throughout the curation lifecycle of digital material.
- Community watch and participation: this is helpful to maintain oversight on appropriate community activities while also participating in the development of shared standards,

tools and suitable software. Furthermore, it helps in development and evolution of appropriate tools and standards.

- Curate and preserve: this action assists to undertake management and administrative actions planned to promote curation and preservation throughout the curation lifecycle

Sequential lifecycle actions

According to Higgins (2011) and Constantopoulos et al (2009), sequential lifecycle actions specify a set of activities that are undertaken in a particular order, so as to facilitate the curation and preservation process. The actions of sequential lifecycle follow below:

- Conceptualise: this is where one plans and conceives creation of data with the inclusion of method and storage options.
- Create and receive: in this action, data is created including administrative, descriptive, structural, and metadata. Receive data in line with documented collecting policies, from data creators, archives, repositories or data centres. Appropriate metadata can be assigned when needed.
- Appraise and select: this action is needed to evaluate data and select for long-term curation and preservation in accordance with the regulatory framework.
- Ingest: data is transferred to archives, repository, data centre or other custodians of data in adherence to the existing regulatory framework.
- Preservation: this action ensures long-term preservation and retention of authoritative nature of data. Data must remain authentic, reliable and usable while maintaining integrity. Included actions are data cleaning, validating, assigning preservation metadata, representation information as well as ensuring acceptable data structures.
- Store: data must be securely stored as prescribed in the standards and regulatory framework.
- Access, use and reuse: data must be accessible to designated users, re-users on daily basis in forms of publicly available published information, access controls and authentication procedures are applicable.
- Transform: this actin provides for the creation of new data from original like: migration to different format and creation of subset by selection or query to create newly derived results for publication.

Occasional lifecycle actions

Various scholars such as Higgins (2011) Constantopoulos and Dallas (2008) and Constantopoulos et al (2009) describe occasional lifecycle actions as activities that are undertaken less frequently, like the disposal of data that have not followed proper curation and preservation guidelines, the appraisal of data that fail current validation procedures for further appraisal and selection and the migration of data to a different format.

The actions that fulfil occasional lifecycle are as follows:

- Dispose: this action focuses on disposing data which has not been selected for long-term curation and preservation in line with documented regulatory framework. Usually, data may be transferred to another archive, repository, data centre or destroyed in some instances. The nature of data may necessitate secure destruction for legal reasons.
- Reappraise: Data that failed validation procedures must be returned for further appraisal and reselection.
- Migrate: data must be migrated to a different format when the old one becomes obsolete or to conform in a new storage. Typically, this occurs when technology evolves where hardware and software become incompatible.

As indicated in section 1.1, digital preservation, storage and disposal are the selected constructs from this model while ingest, create, receive and migrate were intentionally omitted in order to stay relevant to the objectives of this study. It should be noted that the omission does not reduce the roles played by these constructs or the selection of others means these constructs are superior. It should be emphasised that the omitted constructs are key to the definition and the model as a whole. The flexibility of the model allows discussion of each constructs independently to order to add improvement on it in line with situation it is needed for. This can also be realized in the objectives that guide the current study that they are derived from the framework of this study. Again, this is intended to remain focused to the purpose and objectives of the current study. The selection of the afore-mentioned constructs is supported by the assertion of Jing and Fang (2017) that the DCC lifecycle model interprets digital curation as a process of selectively implementing ongoing and systematic maintenance and management of dependable scientific data of reuse value from its creation in line with scientific data lifecycle to confirm reuse and value addition of the data, including a series of activities such as scientific data planning, data creation or collection appraisal and selection, organisation and disposal, description, transformation, storage and reuse. According to Shadbolt et al (2012), its concepts

emphasise the need for access to information and availability of online services. Adu, Dube and Adjei (2016) also state that the concepts' very foundation and survival hinge on the extent to which digital data are preserved. Keeping of records in another way as the manual practice consists of digital preservation in the cloud storage. The documents are converted to digital format and ingested to the cloud storage for easy access by the authenticated users.

1.3 Problem statement

Despite a myriad of potential opportunities offered by ICT where data storage can be hosted in the cloud, Ngoepe (2011), as well as Decman and Vintar (2013) reveal that the national government departments in South Africa continue to keep their records primarily in the form of paper, audio-visual and microfilms in their registries within their premises managed by registry clerks. These records can only be accessed manually by visiting the physical storages, which are often over-crowded. Bekker (2016) contends that in some organisations valuable records are discarded because there is not enough space to store it as the existing database management tools are unable to cater for big data curation, including archiving, management, preservation, retrieval, and representation. In South Africa, the responsibility of regulating government records falls under the auspices of NARSSA, which Ngoepe (2014) argues does not have the necessary infrastructure to manage and preserve digital records. In cognisance of the continuous evolution of technology, records, particularly audio, become obsolete for retrieval because some technological devices are phased out and replaced with recent advanced equipment. Stuart and Bromage (2010) contend that the process of storing information in an organisation is not cost-effective. The expenses can be realised beyond purchasing price for example, licenses per employee, maintenance, add-ons and upgrade costs. Furthermore, the records or software become obsolete. Bearing in mind that records form footprints of the organisations, obsolescence leads to the loss of significant information. Lately, the digital preservation of records is viewed as a way out from paper records given the assurance it provides, for example, reliability (documents as proof of what it is) and authenticity (trustworthiness over time) (Ferreira, Drummond & De Araujo 2017). Advantageously, South Africa has adopted the international standard for archiving, the ISO 14721:2012 Reference Model for Open Archival Information Systems (OAIS) which is applicable to any archive and should be of value to organisations that are accountable for creating information available for longer a period of time.

Some public sector institutions in South Africa have procured systems to manage digital records (Katuu & Ngoepe 2015). Those systems are used only within the local area network (LAN) of the departments where data storage is decentralised and it is accessible to minimal authorised registry clerks. According to Kuiper et al (2015), such practice does not promote the rollout of the e-government service that is envisioned by the government of the Republic of South African. In the presence of a newly introduced cloud computing technology and cloud storage, digital preservation is enabled where users can virtually retrieve data at the same time, but from different locations without interfering with each other. The government needs to address the gap created by the current physical storage of data where access is authorised to limited individuals. Kuiper et al (2014:3) agree that cloud computing provides advantages such as increased flexibility and agility.

Moreover, despite the potential advantages offered by cloud computing, its adoption in the public sector lags behind. Research findings indicate that a take-up of cloud computing services is less than five per cent of the footprint within the public sector (Bellamy 2013). It can be argued that the public sector has interest, but at the same time is sceptical about privacy and security, which amount to public value. Additionally, the current legislation was promulgated without cloud computing in mind, hence government departments retain their autonomy and data storage remains within their premises. Yang et al (2016:1) support the view that cloud storage allows digital preservation, which forms the backbone of e-government services. In view of the above discussion, the South African government departments must take into consideration the advent of technological wheel and review that records are stored in the cloud in order to enhance e-government services.

1.4 Research questions

The study is therefore, guided by the following research questions:

- what legislative frameworks are influencing the storage of information in the cloud in the cloud to support government services in South Africa?
- how can a shift towards storing records in the cloud retain trust towards improving government services in South Africa?
- what are the enablers for the implementation of digital preservation of records in the cloud?
- what are the enabling factors that are followed to dispose records in the cloud?

- which framework can be used for curation of records in the cloud be guided in South Africa?

1.5 Purpose and objectives of the study

The purpose of this study is to explore digital curation of records in the cloud to support e-government services in South Africa. The specific objectives were to:

- analyse policies and legislative frameworks used for records storage in the cloud in order to support e-government services.
- determine if the public sector entrusts records in the cloud storage.
- analyse the public sector's view on digital preservation of records in the cloud.
- determine the processes followed to dispose of records in the cloud.
- propose a framework that guides curation of records in the cloud in South Africa.

1.6 Significance of the study

Kothari (2004) explains that the significance of the study is a manner in which a particular study relates to larger issues and uses a persuasive rationale to justify the motive of the study. Creswell (2013) also adds that it focuses on other ways that augment the academic research and literature in the field, and how it improves practice and policy. The significance of this study is grounded on the fact that other studies on cloud computing did not look at digital preservation of data in cloud computing in support of e-government in the public sector. It is significant because it seeks to store the state's records in a digital place as opposed to the other studies that focused specifically on cloud computing, data storage and e-government. Bwalya and Healy (2010) concur that few studies focused on the issues of access to government information and the adoption of e-government. Theoretically, this study provides an integrated model that explores the migration of digitised records to the cloud for government departments. Practically, the results provide guidelines to the software developers who would be helping the public sector, guided by the proposed framework to expedite access of data stored in the cloud storage. The University of South Africa (UNISA) (2010) indicates that the justification of a study verifies that the study is original by its significance, benefits to the community and its influence to the body of knowledge in the field involved in the study. In relation to this study, it is hoped that encouraging the government departments to store data in the cloud would

promote sharing of information, saving of time and cost, efficiency and effectiveness when providing services to the citizens.

1.7 Originality of the study

Cryer (2006:75) contends that academic institutions require theses to demonstrate originality when researching for a doctoral degree. This author further maintains that some of the factors of originality are as follows:

- The potential of the study to add to the body of knowledge.
- To also be published when the scholar explores an area that is not well known.
- The researcher collects original data.

The reviewed literature points out that research in relation to this study has not been fully explored. Its originality is derived from, amongst others, views of lawmakers, CIOs, and senior records practitioners in relation to the objectives of the current study through interviews. It anticipates to provide guidance on how digital storage could positively impact e-government services. The observation made in delayed provision of services to the citizens influenced by the current records management system informed the originality to this study. This study is developed from a need to simplify the relationship between South African national government departments using cloud services to store records in order to mitigate the current need where records are piling up in a room with minimal access.

1.8 Literature review

Randolph (2009) points out that the purpose of conducting a literature review is a means of demonstrating an author's knowledge about a particular field of study, including vocabulary, theories, key variables and phenomena, and its methods and history. It helps the scholar to avoid reinventing a wheel with regard to answering the questions that have already been answered. Neuman (2011) opines that literature review establishes what is already known about the question before a researcher attempts to find answers about oneself. Bhattacherjee (2012) further postulates that literature review is considered an essential step in conducting a study, because reviewing the accumulated knowledge about a question or questions being researched is very crucial during the research process. For this study, literature on records legislations,

digital curation, cloud storage and e-government was reviewed. This was mainly to reveal the doctrines of literature review of digital curation, cloud storage and the theoretical framework underpinning the current study. It was informed by the objectives of the current study comprising of policies and legislative frameworks; public sector's trust in the cloud storage; digital preservation; disposal of records in the cloud as well as framework that guides digital curation in the cloud. These objectives have been put together into themes and discussed in details in Chapter Two.

1.9 Research methodology and design

Research methodology is a way in which data are collected and analysed (Macmillan & Schumacher 2006:9). Bhattacherjee (2012:35) postulates that research design is a comprehensive plan for data collection in an empirical study. The author further indicates that research design is regarded as a blueprint for empirical research aimed at answering specific research questions or testing hypotheses, and it must specify at least three processes: the data collection, instrument development process and sampling process. This section covers an overview of what is comprehensively discussed in Chapter Three. Table 1.1 provides the research outline and topics covered in Chapter Three as adopted in this study.

Table 1.1 Research outline

Research phase	**Type**
Research paradigm	Interpretivism Constructivism
Research approach	Qualitative
Nature of research	Exploratory
Research method	Case study
Data collection	Interviews and document analysis
Target population selected purposively	CIOs and archive/records practitioners in national government departments
Data analysis	Thematic analysis

1.10 Ethical considerations

Bhattacherjee (2012:137) defines ethics as a normal distinction between right and wrong, and what is unethical may not necessarily be illegal. Creswell (2009:174) expounds that in either qualitative or quantitative research, the scholar is faced with ethical issues that surface during data collection in the field and in analysis and dissemination of reports. According to Johnson and Christensen (2008:109), ethical research embodies informed consent, privacy and confidentiality as well as protection from harm. Bailey (2007:24) states that it is the responsibility of a researcher to assure personal confidentiality of all participants and those participating in a study. This study adheres to UNISA research ethics policy (2010) where a clearance certificate was obtained in order to provide guidance and protection (see Chapter Three).

1.11 Scope and delimitation of the study

This study investigates how digital curation of records in the cloud to support e-government services in South Africa can be achieved. The scope and delimitation of the current study deals with the boundary of what the study would cover (Kothari 2004). While digital curation involves activities that relate to the management and improvement of data from the moment of its generation to ensure availability for rediscovery and reuse of that data in the future, the focus of this study was digital curation of records in the cloud with a view to support e-government in South Africa. The study focused on storage, preservation and disposal of records in the cloud. Other areas of digital curation such as asset management and finance management fall beyond the scope of this study. This study is limited to the CIOs and archive/records practitioners in national government departments. These officials were purposively selected from NARSSA, DTPS, SITA, DST, DHF and DHET. Komba and Ngulube (2012) argue that including a large population in research reduces information overload. According to Komba and Ngulube (2012), qualitative study does not necessarily use a bigger population, but still realise considerable data for use in the study. Considering the qualitative nature of the study, an idiographic approach was followed where a minimal number of sources are used to collect data.

1.12 Discussion of key terms

Yusuf and Chell (2005:28) point out that defining terminology in research is a way to dispel confusion and improves understanding, both for those who are new to the subject and those who are familiar with the subject. The following terms and concepts discussed in this section are explained and expressed according to what they mean and how they are comprehended in the current study:

1.12.1 Digital curation

In an archival space, Post et al (2019) define the digital curation as an "on-going care and attention needed to keep objects viable for present and future, starts from at or before the time of acquisition and continues well after the initial provision of access". These authors also suggest that the long term value of data relies on their potential as evidence, reuse possibilities, role in facilitating compliance and ameliorating risks. On the other hand, Jing and Fang (2017) point out that digital curation refers to "planning, selection, on-going maintenance and display of collections to improve the display rate". The authors further explain that curation involves continuous supplements and updates so that data can satisfy the demand of users. Beagrie (2006) uses this term to "explicitly transfer existing curatorial approaches to digital collections, and also to highlight some of the changes that are needed in approaches to curation of digital as opposed to analogue artefacts (for examples of both transferable practice and changes)." Rusbridge et al (2005) point out that the maintenance, usability and survival of digital resources depends on regular planned interventions; care needs to be taken at conception, at creation, during use, and as use transitions to lower levels. Given that this study has the intention to explore the migration of records to digital curation in the cloud, the definition of Post et al (2019) is relevant to the study.

1.12.2 Cloud computing

Laudon and Laudon (2015) define cloud computing as a model in which computer processing, storage, software and other services are utility-supplied as a pool of virtualised resources over the network, primarily the internet. Literature review indicates that using cloud computing, storage is created in the cloud where data of many organisations can be stored and accessed virtually at the same time from different places. The CSP uses a multi-tenancy model where

cloud consumers share resources in the cloud environment. In the context of this study, records in the form of paper, audio and microfilm are locally stored in registries and are only accessed physically. This study investigates how such record keeping method can be digitised and migrated to the cloud.

1.12.3 Digital preservation

Constantopoulos et al (2009) define digital preservation as a process that ensures long-term preservation and retention of the authoritative nature of data. Preservation actions should ensure that data remain authentic, reliable and usable while maintaining its integrity. In addition, the authors mention that actions include data cleaning, validation, assigning preservation metadata, assigning representation information and ensuring acceptable data structures or file formats. According to Kriesberg (2017), within the public sector, the dramatic increase in the amount of information created and held the by the governments being in the mid-20th century led to increased concerns about preservation and access to the public data as well as the creation of records management in the form of National Archives. Various authors provide the following definitions of data preservation:

- Viana and Sato (2014) define data preservation as the ability to ensure that digital data being stored today can be read and interpreted in the future.
- Conway, Moore, Rayasekar & Jean-Yves (2011) define digital data preservation as an active management of digital information over time to ensure its integrity, authenticity and chain of custody.
- Beagrie and Jones (2001:10) define data preservation as the series of managed activities necessary to ensure continued access to digital materials for as long as necessary, beyond the limits of media failure or technological and organisational change.

The definition provided by Beagrie and Jones (2001) is appropriate for this study. This is informed by the way it enhances the managed activities that are necessary to ensure continued access to digital materials for as long as necessary, beyond the limits of media failure or technological and organisational change.

1.12.4 E-government

E-government is a use of ICT to improve information sharing, delivering online services to citizens and facilitating interaction between governmental agencies and outside stakeholders (Wahsh & Dhillon 2015). Despite various definitions given for e-government, the common theme is that e-government requires the internet in order to perform. The United Nations defines e-government as a way of utilising the internet and the World Wide Web (WWW) for delivering government information and services to citizens. Mohammed, Ibrahim and Ithnin (2016) state that e-government is a generic term for web-based services of agencies of local, state and federal governments.

1.13 Structure of the thesis

This section provides an overview of how the entire study will be structured. Comprehensive discussion is available on the chapters that are summarised below.

Chapter One: Moving away from traditional record keeping to digital environment
This chapter provides the introduction and background, theoretical framework, problem statement, purpose and objectives of the study, significance of the study, originality, research methodology and design, ethical considerations, scope and delimitation, as well as discussion of key terms of this study.

Chapter Two: Literature review on digital curation in the cloud storage
This chapter discusses literature review and applied theoretical framework that underpinned this study. Guided by the theoretical framework, literature was reviewed based on the research objectives.

Chapter Three: Research methodology
This chapter presents the research methodology followed to conduct this study. It discusses research paradigm (epistemology and ontology identified as interpretivism and constructivism), research approach (qualitative), nature of research, research methods (case study), data collection instruments (interviews and document analysis), as well as ethical consideration, data trustworthiness and research evaluation.

Chapter Four: Data analysis and presentation of findings

This chapter presents the findings collected from the target population through semi-structured interviews and document reviews. The presentation of the results is guided by the objectives of the study which are organised according to the themes. It concludes with the actual words of the interviewed participants to express ideas as they were captured.

Chapter Five: Interpretation and discussion of findings

This chapter provides the interpretation and discussion of findings from Chapter Four. The results are interpreted and presented based on the research objectives of the present study.

Chapter Six: Summary, conclusions and recommendations

This chapter revisits the research objectives of this study in order to present the summary, conclusions and recommendations based on data findings and data presentation in Chapter Four and Chapter Five. It provides conclusions of the investigation and organises them according to the objectives of the study. This section proposes recommendations to address issues identified during the study. The recommendations address each of the research objectives of the current study and a framework is proposed. This chapter presents implications for theory, policy and, finally, makes the suggestion for further research.

1.14 Summary

This chapter presented the introduction and background to the study, literature review and theoretical framework, research design and methodology, presentation of findings, interpretation and discussion of findings, and provided conclusions and recommendations. The next chapter discusses theoretical framework and literature review of this study.

CHAPTER TWO

LITERATURE REVIEW ON DIGITAL CURATION IN THE CLOUD STORAGE

2.1 Introduction

Chapter One introduced, amongst others, the background, problem statement, and research objectives of this study. The current chapter presents literature review, which according to Neuman (2013) facilitates the development of theory and closed areas where there is a plethora of research, discovers areas which are necessary to reconsider and provides an important contribution to the establishment of guidelines for future research that is fundamental to the strengthening in the area of the study. As indicated in the previous chapter, the purpose of this study was to explore digital curation of records in the cloud to support e-government services in South Africa. It is in line with a vision of the South African government of improving government performance through e-government services. The significance of this chapter is to reflect the link between objectives and theoretical framework underpinning this study. This is informed by the fact that the South African government departments still have data on their premises, prominently in paper, film and audio formats, which does not promote online access. Despite all that, it is anticipated that with cloud storage, national government departments would access data seamlessly as opposed to the paper-based records management.

2.2 Purpose of literature review

The purpose of literature review is three-fold: (a) to survey the current state of knowledge in the area of inquiry, (b) to identify key authors, articles, theories, and findings in that area, and (c) to identify gaps in knowledge in that research area (Bhattacherjee 2012:22). It is a body of text whose purpose is to review the critical points of current knowledge, including substantive findings, and theoretical and methodological contributions to a particular topic. Literature review offers numerous benefits which include new ideas, revealing data sources which a researcher might be unaware of and indicating how other researchers handled methodological design issues that were applied (Leedy & Ormrod 2013:51). In the same breath, Neuman (2013:124) reminds researchers that thorough homework should be done around the topic before conducting a study in order to avoid reinventing the wheel. It is necessary for researchers to review literature, especially or including the completed studies at doctoral level in a similar

field of study that has a potential to give direction on the need to cite sources, as well as the proper referencing style that should be used. Maluleka (2017) posits that the more the scholars know about the investigations and perspectives related to the topic, the more effectively they can address the research problem in hand. Neuman (2013) and Leedy and Ormrod (2010) agree that literature review permits researchers to pay attention at the debates and arguments made by fellow researchers in relation to a topic under investigation. Furthermore, Creswell (2013) expounds that it is considered as a critical summary and assessment of the range of existing materials dealing with knowledge and understanding in a given field. It gives an opportunity to researchers to establish the conceptual framework within which the study is located. In this regard, a number of studies were referenced in order to establish the importance and viability of the research objectives.

In order to identify gaps, this study used a variety of sources in the form of books, journals, government publications, conference presentations and websites in order to conduct successful research. Maluleka (2017:19) encourages researchers that given the relevance of the theoretical framework and literature review, it becomes easier to identify research approaches, methods and instruments applied in related studies. With the advice highlighted by the researchers, the mind of a current researcher was prepared in terms of knowing the relevant literature and theoretical framework to be reviewed in line with the objectives of this study.

2.3 Legislative framework and policy for data storage in the cloud

Digital storage should have a standing legislation within the government to enable implementation all over government departments. This is to ensure that the DCC Lifecycle model is applied in relation to the legislative framework of the country, particularly in the sphere of digital record keeping. The DCC Lifecycle model on its own identifies curation applicable across the whole digital lifecycle. Digital storage forms the memory of the world due to its easy access. In line with this study, legislation and policies advance digital storage, digital preservation and digital disposal of digital records which in turn become the memory of the world. Section 32(1) of the Constitution of the Republic of South Africa (Act No. 108 of 1996) (Constitution) stipulates that “everyone has the right of access to records or/and information held by the state and any information held by another person that is required for the exercise or protection of any rights.” Rogers (2015) supports this Section 32((1) by pointing out that the ability of citizens to access the government’s information fully and in a timely

manner is considered one of the cornerstones of democracy. It is an indication that citizens' rights and government's accountability depend on how records are created, managed as well as preserved. Peekhaus (2011) also encourages that the South African societies deserve access to information as provided in the legislation. Furthermore, the Constitution has permitted the national legislation to establish the general policy framework by which governmental bodies should operate to ensure effectiveness and efficiency of information. The International Standard of Records Management stipulated the following five levels within the regulatory environment: statute and government regulations, mandatory standard of practice, voluntary codes of best practice, voluntary codes of conduct and ethics as well as community expectations. Having looked at the theoretical framework and to stay relevant to the study, this section discusses legislative frameworks and policies, respectively, in relation to records storage in order to support e-government. Legislations and policies are applicable in both paper-based and digital storage environments.

2.3.1 Legislative frameworks governing data storage in South Africa

According to Mittal (1971:4) and Jackson and Shelly (2012), legislation means laying down instructions for the persons responsible for running a government in order to properly discharge each function of government. In line with the theoretical framework, Mutkoski (2015) advises that digital storage should be informed by the cloud legislation to allay fears of loss of information when the public sector considers migrating records to the cloud. Indeed, Stančić, Rajh and Jamić (2017) confirm that due to the influence of ICT, the archival processes are affected. Ngoepe and Saurombe (2016) opine that to enable the proper management and preservation of digital records, there is a need for an archival legislation to embrace records created and stored in the networked environment, such as cloud storage. Ngoepe (2014) and Ngoepe and Nkwe (2018) establish low uptake of cloud storage in South Africa owing to the issues such as a lack of guidelines and legislation regarding cloud computing. This is essential in cognisance of adopting cloud computing where the public sector as a main focus of this study should be familiar with South African regulatory requirements, legislation and policies.

According to Ngoepe and Saurombe (2016), legislation has a tremendous impact on how records are stored in networked environments in any country. These authors also contend that in African countries, technological development is moving faster than the corresponding legislative framework. On the other hand, in countries such as Canada and Australia the gap

between the legal system and the digital world is not as big since there have been studies that are dedicated to narrowing the gap (Ngoepe & Saurombe 2016). In South Africa, government departments tend to use technology without applicable legal documents. The International Records Management Trust (2015) provides that the enactment and implementation of comprehensive, up-to-date archival legislation are a critical prerequisite for the establishment of an effective, integrated system for managing records. The archival legislation provides the essential framework that enables a national records and archive services to operate with authority in its dealings with other organs of state (Ngoepe & Saurombe 2016). The legislative framework protects the storage of records in various formats, for example, paper, audio and microfilm. Franks (2013) states that the statutes that originate from legislative bills create legal frameworks. The legislative items determining the records storage framework in the South African government as published on by the National Archives of South Africa are: Constitution of 1996, NARSA Act (No. 43 of 1996), Promotion of Access to Information Act (PAIA) (No. 2 of 2000), Electronic Communications Transaction Act (No. 25 of 2002) and some International Organisation for Standardisation (ISO) which have been endorsed. These Acts are an indication that legislation on digital storage has not been promulgated. This means one has to read various pieces of legislation in order to come up with the cloud information. The NARSA Act of 1996 clearly advocates for the storage of paper-based and digital records in a securely locked environment within the government premises.

Dependence on this Act has a negative impact to the community that should access records from where they are. The directives of the Constitution to develop legislation that has its proximity of cloud storage has have ignored or delayed. The NARSA Act of 1996 stipulated that in terms of its statutory mandate, “governmental bodies are required to put the necessary infrastructure, policies, strategies, procedures and systems in place to ensure that records in all formats are managed in an integrated manner”. For example, every organisation is expected to identify the regulatory frameworks that affect its activities and requirements in order to document the activities. This is influenced by the fact that storage is a memory of an organisation that provides evidence that should be protected by legislation and policies of a government. Various researchers such as Kemoni and Ngulube (2007), Keakopa (2010), Kalusopa (2011) and Kalusopa and Ngulube (2012) suggest that best practice for records management means that organisations should provide adequate evidence of their compliance with the regulatory environment in the record of their activities.

In the same breath, Assefa (2001) and Reif (2004) mention that the governance elements are: "effective management of public sector administrative procedures; treasury controls; mechanisms to monitor financial and accountable use of resources; and civil rights to all people living within the borders of the country to fair, equal treatment and public participation in governance processes." At this moment, one needs to read various pieces of the afore-mentioned legislation in order to come up with cloud-related information.

Findings by Ngoepe (2012) affirmed that the government records are prominently stored in the form of paper media, audio and microfilm, which are securely locked in the safe area of government premises. The paper-based secure storage is precipitated by the fact that the NARSA Act No 43 of 1996 was promulgated before the network infrastructure became pervasive. On the other hand, it was relevant to manually keep records so that when technology arrived, they would be easily collected in organised places for digitalisation according to their categories. According to Shen et al (2012), today's IT network infrastructure, including telecom, cable, internet and wireless, is converging into one standard governed by the cloud. Arguably, the cloud too should have legislative frameworks it should adhere to. The international standards like ISO15489, ISO15489 Records Management Standard, ISO23081 Metadata for Records and ISO15801 Trustworthiness and Reliability of Records Stored Electronically form a prominent requirement to manage electronic documents, records and archives. One other crucial ISO standard used within the records management space for IT security standards, the ISO/IEC 27001, which defines requirements and procedures for the implementation, maintenance, and improvement of Information Security Management Systems (ISMSs) has offered IT security certification since 2005, and a 2013 revision brought it up to date with new technologies. This ISO provides security in the form of certification to the consumers that use virtual environment. The international standards alone cannot be relied on without the support of the legislation. Furthermore, the IT infrastructure has matured enough to support cloud storage legislation for the benefit of all consumers, irrespective of their area.

2.3.2 Policies for digital storage in the public sector

The policy on digital storage must be linked with the NARSA Act in order to ensure that records meet compliance. Central to the effective records management policy is that it should be tied closely to the business processes that create the records that are documented. The findings by Ngoepe (2012) pointed out that records management policies must list the

following characteristics of policies: good governance, accountability, transparency, responsiveness, participatory, adherence to the rule of law, effectiveness and efficiency. Furthermore, Kriesberg et al (2017) mention that some agencies with long history of supporting and conducting science, have taken steps towards implementing compliant policies in their organisations.
The International Council on Archives (ICA) defined policy as mandating practices within a specific individual organisation or group of related government organisations. Policy is an action that employs governmental authority to commit resources in support of a preferred value (Considine 1994). Policies form part of governance, which involves interaction, impact and functions of the state and its officials with its citizens and the people who live within the borders of that country (Cook 2001:19. Furthermore, ISO 15489-1 (2001:7) reflects that policies should stipulate the requirements for capturing, registering, classifying, retaining, storing, tracking, accessing and disposing of records. Contrary to the statement of Ngoepe (2012) that each government has its own paper-based registry whose policies correlate with the NARSA Act, this method does not enhance distant communities to gain access to the records at their own time. The communities travel to the premises in order to access records. Should there be unexpected events such as labour unrest or other activities that affect operations, travelling to the premises would be futile because they might go back without achieving the goal of visiting the premises. If the records were stored in the cloud, through e-government services the citizens would conveniently gain access to the records at their own time and place. Information governance should take a centre stage in the cloud storage and the records stored in it.

The Institute of Directors Southern Africa (IODSA) 2016 points out that technology governance and security have become significant in the technology spheres Technology has gone beyond the level of an enabler of thee of the organisation, it has become both the source of an organisations' future opportunities and of potential disruption, an excellent example of how risk and opportunity are increasingly two sides of the same. IODSA adds that the security of information systems has also become essential .critical. This is one other reason the general IT controls (GITC) (2018) indicated that these controls should be in utilize cloud and e-government services. According to IDIOSA and Deloitte, GITC are controls that apply to all systems, components, processes and data for a given organization or IT environment. GITC provide the foundation for reliance on data, reports, automated controls and other system functionality underlying business processes. According to King IV 0f 2016, the most common ITGCs are:

- Logical access controls over applications, data and supporting infrastructure

- Program change management controls
- Backup and recovery controls
- Computer operation controls
- Data centre physical security controls
- System development lifecycle control

Significantly, one of the key principles of ICA is that institutions holding archives must adopt-pro-active approach access. The national archivist should maintain a professional responsibility to promote access to archives. Doran (2012) and the National Archives and Records Administration (NARA) (2010) shared a similar view that records management in government serves a crucial role in support of the delivery of government services, providing evidence of the government transactions, as well as legal and regulatory obligations.

NARA (2010) outlines that records generated in government possess historical value, and are necessary to secure the rights and privileges of citizenship. The legal and regulatory requirements have clarified the need for governments to control both electronic and non-electronic information within their policies (Doran 2012). Information governance framework relies first and foremost upon a comprehensive records and information management policy that draws on the best practices and can be adapted for almost any circumstances (Franks 2013). The organisation is healthy when its bureaucratic processes and functions are in order. The effective management of records is fundamental to the efficient running of bureaucracies (Katuu & Ngoepe 2015). Policies provide the framework for archival records, but implementation is at the recordkeeping system level (ICA 2005). The ICA (2005) further points out that the archivists must work with decision makers to support both records management and archival programmes.

2.3.3 Digital storage policies in selected countries

Every state worldwide has consideration for a value of data storage whose policies are guided by their national archives services. Those policies are conversant with the digital and paper-based archives. Thurston (1996:187) observes that national archival institutions in Africa have a statutory responsibility for records management in the public sector and any attempt to understand the development of records management in the public sector in Africa needs to

focus on the national archives. The earlier discussion revealed that the international standards for the development of records management programmes (ISO15489-2 Information and document record management Part II) remain emphatic on the importance of records management policies and support for records management from senior management of an organisation (ISO 2001). In many countries, including South Africa, the national archive institutions are mandated by the records and archives legislation that defines the proper management of records in the public sector.

In the United Kingdom, the National Archives (2004) advised government departments and the wider public sector on the best practices in records management. To improve trust, the government has developed a secure cloud infrastructure, Government-Cloud (G-Cloud) to be used by public sector bodies. Significantly, this strategy provides standardisation for capabilities of shared services with accredited cloud service providers, which helps to reduce public sector spending. In Australia, the National Archives (2004) provides advice to government agencies by developing policies, standards, and guidelines, and providing training and advice about modern record keeping. In the United States of America, the National Archives and Records Administration (2004) helps to preserve the history of the nation by overseeing the management of all federal records. According to NARA, the Records Management Policy and Outreach Program, under Office of the Chief Records Officer develops Federal records management policies and guidance related to records creation, management and disposition with an emphasis on electronic records. This, propels a proper regulation of digital records that are accessible regardless of distance. Generally, the countries in Europe, Asia and America are considered to be ahead in terms of technology. For instance, the USA is considered the best consumer of cloud services while Asia, particularly China is the biggest producer of technology. African states have been selected given that they are considered as the developing countries. The National Archives of India (2005) has engaged in streamlining the management of public records. The government of Botswana (2007) points out that the mission of the Botswana National Archives and Records Services Department (2009) is to provide efficient and effective economic management of all public records throughout their life cycle and to preserve those public records of archival value for posterity and access purposes. Lastly, in Kenya, the Kenya National Archives and Documentation Services advises public offices on the proper management of records.

2.3.4 Benefits of policies in the digital storage

Appropriate records management is an important aspect of maintaining and enhancing the value of the asset of the organisation. NARSSA (2007) points out that in the Republic of South Africa, the current record management policies promulgated by the public archivists support the role performed by all these players in the creation, management, identification and preservation of information sources. However, in order to achieve that, NARSSA (1997) stipulates that the prescribed national archives' registry procedure manual guides the records practitioners rendering services in the registries of South African public sector. Furthermore, NARSSA (1997:2) indicates that the prescribed manual assigns the duties of the administration and supervision of all registry procedures, supervision of registry, training as well as all related delegated record management tasks to the chief registry officials. For this reason, the government departments have their registry sections operate in line with NARSSA.

According to National Archives' Records Management Policy (NARSSA 2004; 2007) and Performance Criteria for Record Managers of Government bodies (NARSSA 2004c), such officials manage the activities of records practitioners as well as all other related areas involved with the management and care of information sources generated and received by the entity. NARSSA (2004c) clearly states that record managers are responsible for the control and access to information sources while they remain in the current and semi-current stages within the jurisdiction of the creating entity. To date, the State Archives Act (No. 6 of 1962) (South Africa 1962) outlines that the records management component of present day NARSSA is required, in terms of the related parliamentary Act, to perform the same functions as at its inception in 1957.

2.3.5 Risks of operating without records management policies

It is an enhancement of governance for government departments to develop a records management strategy that informs records management policy. It should regulate records management activities, procedures, retention schedule, vital records schedule, file plan and business continuity. Ngoepe (2017) argues that in South Africa, the responsibility of regulating government records to support e-government falls within the auspices of NARSSA, but necessary infrastructure to manage and preserve digital records is non-existent. Ngoepe (2012) highlights that failing to manage the records throughout their life cycle is a risk facing every

organisation. The author argues that failing to implement records management policies and carrying out disposal authorities, governmental bodies would not be able to meet the legislative or other obligations required of them. “The government archives provisions how records should be correctly managed in government offices, conducts inspections at the offices to determine and advise on responsible record-keeping practices, and advised on the use of record classification systems” (Davies 1960). Indeed, these services were performed by the archival staff, while performing other archival tasks like arrangement and description of archivalia, compiling inventories and related finding aides, handling transfers of archivalia to repositories and assisting researchers.

Ngoepe (2014) indicates that the workers responsible for archives in government are marginalised clerks. The officials within that section are considered non-essential because their functions are associated with filing records. It is quite easy to empower other sections and leave registry officials because their functions are deemed as something that anyone can do without particular expertise. In support of the finding, the *Daily Mavericks* (1 May 2019) reported that marginalisation stretches from the appointment of political heads of the Department of Arts and Culture (DAC). The NARSSA forms part of the DAC. The *Daily Mavericks* (1 May 2019) indicated that the appointment deepened the perception of the DAC as a dumping ground for under-performing or politically radioactive ministers of a ruling party, and that has extended to the registries of each government department. Despite their benefits, Yakel (2006) suggests that government archives face a number of challenges in today’s public sector. When Minister Nathi Mthethwa (2014 present) was appointed to the role of arts and culture from the police portfolio in 2014, it is perceived to be a political demotion. The minister was embroiled in a number of political scandals, chief among them was the poor handling of Marikana Massacre under his watch as the Minister of Police in 2012. Any appointment in the DAC is viewed as a demotion, because the DAC’s political capital is deemed to be low. In stark contrast, the policy has stipulated the level of qualification that such people should have, but that is not practised. This call was made in line with section 91(3c) of Chapter Five of the Constitution, which permits the president to make no more than two Cabinet appointments from outside the ranks of the National Assembly. This would lead to the appointment of a suitably qualified head of the department who would understand the archives and records management. Nevertheless, Franks (2013:33) suggests that organisations have been looking to records and information programmes in order to mitigate risks to the organisations. Such approach was concerned with

what would happen in the absence of comprehensive records management programme. In the absence of comprehensive records programme, the following major concerns reflect:

- Damage to the organisation's reputation
- High costs of information management and storage
- Lost files and risk of spoliation
- Legal discovery penalties or sanctions
- Audit and compliance violations

Franks (2013) holds that an effective records management programme comprises records management policy and procedures, well-trained personnel, and advanced information systems which reduce the risks within the records management environment. Given that many government departments are still prominently using a paper-based records management system, it is quite easy for the documents to disappear due to the continuous piling up of papers. The NARSA Act states that the departments have their filing system that guides storage as well as access to those files. As records management forms a strong memory of the organisations, Bhana (2008) and Ngoepe (2011) list legal, financial, reputation and information problems as the prominent risks that could be experienced due to lack of proper record keeping. Additionally, the filing system provides the storage according to the media format, for example, paper, audio and microfilm. As a risk, Ngoepe (2012) espouses that in terms of the Promotion of Access to Information Act (PAIA) (No. 2 of 2000), they would be struggling to sift through an ever-increasing mountain of records. The author further points out that the head of department and top management team endorse the effectiveness of records policies and are supported by key records management documents like file plan and procedures. On the other hand, the same cannot be said when digital records policies have been developed to guide digital records.

2.4 Storage of records in the cloud

According to Higgins (2008), data should be stored in a secure manner that adheres to relevant standards. This section discusses cloud storage and determines if public sector entrusts cloud storage.

2.4.1 Evolution of cloud storage

According to the ICA (2005), the evolution of technology developed systems used for records creation and records management. Such systems perform some of the following functions: storing, retrieving, sharing, preserving and many more. The ICA (2005) also contends that these systems include standalone and non-networked systems. However, this study focused on a modern record storage environment, the record-keeping system that involves distributed networked environment levels. According to Ning et al (2015), the examples are client-server environment within an organisation, sharing applications and services by decentralised workstations, intranet and internet-based information network where various organisations participate in the sharing of digital records. This explains that the record-keeping system should be an instrument that governs records management functions through the entire life cycle continuum. Cloud storage contributes to the enhancement of access to computing resources for enterprises interested in the development of a robust IT infrastructure in developing countries where the possibilities of doing so can be difficult (Dahiru, Bass & Allison 2014).

Sprott (2012:7) points out that cloud computing was used as a metaphor for the internet. Jamsa (2014:65-66) mentions that long before the introduction of cloud computing, workgroup network and LAN, some of the organisations used file servers to support file sharing, file replication and storage for large files. Through the evolution of computer networks, file servers were extended to storage area networks (SANs), which could make one or more storage devices that were directly connected to the network. Due to the continuous demand for data storage, the network attached storage (NAS) emerged. It should be noted that both SAN and NAS storages did not address a broader access to file sharing, because they were confined to the LAN of that specific organisation. This is because data could only be accessible on premises by those who had the credentials of that organisation's LAN while onsite or through a virtual private network connection (VPN-C). This study contends that the methods used could not fulfil data storage that enabled the implementation of envisioned e-government services for the South African government.

Following the NAS device, the cloud storage emerged in order to provide virtual access of information to anyone from anywhere at any time. Most of the private companies such as Google, IBM, Microsoft, to mention but a few became cloud service providers. Small, medium and large enterprises pay subscription fees for virtual servers in order to store their data. Yang

(2012:4) argues that in reality, customers share the same physical machine with many other customers. Since its inception, it has become huge mainly in developing countries (Jamsa 2014:65-66). Colicchio, Giovanoli and Gatziu (2015:177) note that the adoption rate of cloud computing is not growing as expected. Furthermore, that is influenced by the fact that the main infrastructure (internet) for successful implementation of cloud computing is not well structured or the infrastructure still needs improvement to support cloud computing in other countries. Given the widespread use of internet, Assyne and Riungu-Kalliosaari (2014:1) argue that cloud computing is popular in developed countries as opposed to the developing countries where only few institutions are accessing their services and records in the cloud. According to Colicchio et al (2015:177), some examples of cloud-based storages are Dropbox, Box, Google Drive and many more, which customers use for file sharing. These types of tools are appealing to the new generation of users who like to collaborate and to synchronise files directly from their mobile devices. Jamsa (2014:67) lists the following ways that can be used to access data on cloud storage:

- Through a web browser interface that lets users move files to and from the storage area using a variety of devices
- Through mounted disk drive that appears locally to the user's computer as a disk drive letter or mounted file system
- For application developers, the storage area may present itself through a set of application program interface (API) calls

2.4.1.1 Models used for cloud computing services

Reza Bazi, Hassanzadeh and Moeini (2017:88) and Mohammed et al (2016) share a similar view that cloud computing comes in the following three types of service models, namely software as a server (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS), that are hosted by cloud service providers, and all of them are accessed using the internet as communication channel. Asaeed and Saleh (2015) suggest that the organisations can choose the deployment models in order to deploy private cloud, community cloud, public cloud and hybrid. Garcia-Galan, Trinidad, Rana and Ruiz-Cortes (2016) argue that it is difficult to select an appropriate configuration for infrastructure, best service and provider. On the other hand, Van der Schyff and Krauss (2014:40) suggests that utilising cloud computing requires users and organisations to trust cloud providers. Contrary to the telephone and electronic mail system

where the persons identify each other, the widespread of cloud coverage makes it unnecessary to know the persons that the consumers are dealing with or who is handling the records. IT managers are required to have a clear understanding of technology, its advantages and its usefulness in their business operations in order to select the one that best fulfils the needs of the organisation (Gangwar, Date & Ramaswamy 2015:108).

Since cloud computing is managed by the CSP at its premises and accessed through the internet, cloud computing makes it easier to reduce functionalities like data centres managing software applications, allowing the organisation more time to focus on strategic issues like policy development, public service design and delivery (Mohammed et al 2016:303). In the absence of machines for data storage on the premises of the client, for example, government departments, power (utility) and resources (IT technicians) are required in less demand. The service models, which are considered the first step to be taken when migrating to the cloud, are discussed below:

(a) Software as a Service

SaaS is a model where software and other solutions are delivered to the end-users as a service using the Internet rather than as a product that can be installed on users' computers or mobile devices (Park & Ryoo 2012:161). Han (2013:88) agrees that SaaS allows users to use CSP's applications on cloud through a web browser or API. This model has been designed in a way that a CSP manages almost everything in the cloud infrastructure, for example, physical servers, network, operating system and application. The most common examples are Google Drive, Dropbox, Sky Drive and Google Docs where one can upload documents and collaborate or use a form to create online surveys (Han 2013:88; Yang 2012:4). Its flexibility allows users to have more control, because it is hosted on the local server where all the system administrators' work is done locally such as backup and troubleshooting. Maintenance remains the responsibility of CSP. Sprott (2012:10) argues that the ease with which the SaaS application can be purchased has made this model the most widely adopted service.

(b) Platform as a service

PaaS is an extension of SaaS and provides a platform to build and run application packages using an API that is supported by CSP (Polyviou & Pouloudi 2015). Despite customers having

control over their installed applications, they do not manage or control the core infrastructure like hardware, software and storage (Sprott 2012:10). Yang (2012:4) points out that PaaS allows users to deploy their own application to the providers' cloud infrastructure under the CSP's environment such as programming languages, libraries and tools. Program developers often use PaaS to develop and test new programs.

(c) Infrastructure as a service

Reza et al (2017:88) suggest that this pay-as-you go platform allows an organisation to outsource its whole IT infrastructure to a CSP in support of its day-to-day operations such as servers, software, technical support and storage (Sharma & Banga 2013). It allows users to control or manage computing resources like storage, networks and computing power so that they can deploy and run arbitrary software. Mohammed et al (2016) point out that users have maximum control of the infrastructure as if they own the underlying physical servers and network. This model allows customers to buy a software solution as a service and not a product. It is capable of attracting many organisations because of its flexibility to manage their service demand and it helps them to access the latest networking technology at a much lower cost. This model is commonly known for preservation of data.

2.4.1.2 Cloud deployment models

Since technology is not one-size-fits-all, cloud deployment models provide a range of models that CIOs can choose in order to guide the organisation to adopt cloud computing. This is informed by the traditional practices of the organisation. Irrespective of the selected deployment models adopted, NARSSA must remain in control of the government's records. According to NARA, the differences between models affect how and by whom records management activities are performed. This section discussed the four cloud deployment models such as public, private, hybrid and community clouds that are used to deploy cloud platforms.

(a) Public cloud model

Public cloud is a deployment model that is accessible to anyone and is deemed to be less secure due to its openness (Bhandari, Gupta & Das 2016). Some examples of public cloud are

Microsoft Azure, Google Cloud as well as Amazon. Mvelase et al (2013:150) contend that the term public does not always associate with free, despite being fairly cheap. This service model is suitable for smaller and growing organisations that cannot afford the IT infrastructure due to financial constraints. The public cloud provider has the security mechanism in place for the users. The users are expected to register and create user credentials when they use it for the first time. Sarkar and Kumar (2016) espouse that this infrastructure is hosted at the CSP's premises and there is no way a customer can view the infrastructure. Despite the customer using this deployment model with a low degree of control, Sprott (2016:10) argues that it still offers enhanced data efficiency and cost-effectiveness.

(b) Private cloud model

Private cloud is dedicated to organisations where the computing infrastructure cannot be shared (Sarkar & Kumar 2016). Considering that the organisation or third party on or off site can manage it, it is more appealing to the organisations that require more control over their data and additional IT infrastructure investment (Sprott 2012:10). This model has a very strong security mechanism. The CSP is always in control of the data centre where the users' data are stored. The key technology used for private cloud computing is called virtualisation, which helps organisations to realise cost savings through leveraging their existing IT infrastructure and mitigate purchasing additional equipment. As opposed to public cloud, which is hosted at the premises of the CSP, private cloud resides at the customer's location and offers more control over the infrastructure.

(c) Hybrid cloud

This model is an amalgamation of public and private cloud models where some resources are hosted and controlled externally by a third party while some resources are used only by the organisation (Asaeed & Saleh 2015). According to Bhandari et al (2016), this deployment model separates non-critical activities that are performed in the public cloud and critical activities that are performed in the private cloud. Sarkar and Kumar (2016) view hybrid cloud as private cloud that can be extended to use resources in public clouds where organisations submit a less valued application in public cloud and high-valued applications in the private cloud. These researchers indicated that this deployment model helps organisations and businesses to take advantage of data hosting and secured applications on private cloud while

still enjoying cost benefits by keeping applications and shared data on public cloud.

(d) Community cloud model

Community cloud is the deployment model shared by organisations of the same community (Sarkar & Kumar 2016) that has shared concerns, for example, mission, security requirements, and compliance considerations (Kabata 2012:139). Bhandari et al (2016) argue that community cloud is not really a deployment model since it is like private cloud in which systems and services are accessible to a group of organisations. It may be organised and controlled by a third party and it may exist on the premises and off site. The data storage on cloud computing is significant for its capability to keep data where every department can access it to support e-government. Based on the framework and objectives, the security of data should be guaranteed when stored or accessed.

2.4.2 Relationship between cloud storage and e-government

Having discussed the legislative framework in relation to data storage, this section discusses how cloud storage relates to e-government services. Hashemi, Monfaredi and Masdari (2013) postulate that the effectiveness of e-government is reliant on successful implementation of cloud computing. This is informed by the fact that the use of ICT enhances the service quality and efficiency while trimming down on storage expenses.

Sarkar and Kumar (2016) suggest that although there are several types of service models that provide the cloud services, storage of data is one of the latest features. It is a potential means to simplify the ways of accessing e-government services between G2G and G2C. Effective and operational e-government service facilitates a more efficient delivery of information and services to citizens. According to Kim, Kim and Lee (2009:42), time productivity is promoted among civil servants, as it encourages the participation of citizens in government and provides a means for citizens to feel and effectively be more empowered. Kaliannan, Awang and Raman (2009) demonstrate that the adoption of ICT in the private sector such as banks has emboldened the introduction of electronic commerce (e-commerce) and electronic banking (e-banking) where customers process transactions without visiting the bank branches. The authors indicate that consequently, many governments have invested huge amounts of money in developing IT infrastructure and deploying the use of IT to serve their stakeholders in an efficient and

effective way. They also indicate that the initialisation of e-government presents a way for governments across the world to provide citizens, businesses and other governments with convenient access to government services and opportunities to collaborate as well as political participation via the internet and wireless communication technology.

This is motivated by the opportunities that are embedded in ICT towards increasing efficiency in internal processes and offering better services to citizens (Mohammed et al 2016). The authors held that the governments that ignore the value of emerging ICT might suffer significant disadvantages in improving service delivery. However, based on the required infrastructure that supports it, Ebrahim and Irani (2005) argue that the implementation of e-government is costly. Al-Rashidi (2013) and Garcia-Galan et al (2013) indicate that ICT infrastructure, human resources and financial services are the most challenging of e-government in developing countries. Mohammed et al (2016:298) observe that the need to exploit opportunities creates new emerging ICT and paradigms. Cloud computing provides a good basis from which some of the traditional challenges like automated processes are addressed. Literature review revealed that cloud computing has key characteristics and feasible features that make it proper for use in e-government implementation. It is able to remove barriers of access to users, irrespective of their location and time. Mvelase et al (2013:149) support that since it is growing bigger every day, many originations are integrating it into their operations for its cost-effectiveness, maintenance and data storage, which provide digital preservation. While considering migration to the cloud for e-government purposes, applications based on current security practices should be enforced to ensure that they are compliant with security with up-to-date patches, guiding legislations and policies (Bettacchi et al 2017).

Liang et al (2017) views e-government as an administration system in which governments offer full use of modern technology. Zhang (2014) asserts that the inventive objective and eventual goal of e-government is to deliver offer expedient public services. The critical products of government that are most distributed in the form of policies, management information, regulations, markets and the environment require support for digital preservation infrastructure in order to exploit e-government to the fullest (Wimmer 2004).

2.4.3 Cloud computing and e-government services in other countries

Despite the fact that this study focused mainly on South Africa, it is worth looking at how other countries benefited from improving the public services through ICT. According to Ning, Xiaoshan, Li hui, Xuehua and Xuezhi (2015), many countries around the world learnt that the traditional data centres could not afford mass data storage and processing. Furthermore, it was realised that traditional data centres like in South Africa have such poor scalability and lack effective maintenance that they cannot provide reliable decision-making support for the government (Wai-Ming, Lai & Chung 2013). Tao et al (2014) indicate that the emergence of cloud computing globally has provided opportunities for solving the massive e-government data storage problems.

For this study, the following countries that are considered big economies and leaders in ICT consumption were selected in order to ostensibly compare and benchmark what South Africa should consider: United States of America, United Kingdom and China. Reasons for selecting these two countries are informed by their internationally recognised influence in the fields of cloud computing, records management and e-government. The United States of America is the biggest producer of cloud technology while China is the biggest consumer of cloud computing. For this reason, Wang and Zeng (2009) support that e-government in the governments of countries such as china is a way for governments to use the new technologies to provide people with more convenient access to government information and services, to improve the quality of the services and to provide greater opportunities to participate in the democratic institutions and processes.

2.4.3.1 Cloud computing and e-government services in United States of America

Rutrell (2010) mentions that Miami in the United States of America has successfully moved the public telephone service cloud through Windows Azure in order to achieve real-time service. Being the most dominant industrialised countries in the world, the United States of America considers e-government as a vibrant and expanding phenomenon, which offers much to traditional administration in the public sector. Initially, e-government was viewed as an uncertainty, but now has moved to one of the stable interactivities for governments and their citizens.

2.4.3.2 Cloud computing and e-government in China

According to Wai-Ming et al (2013), cloud computing advocate Tom Leighton predicted that the cloud will "transform the way IT is consumed and managed, with promises of improved cost-efficiencies, accelerated innovation, faster time-to-market, and the ability to scale applications on demand. While the market is abundant with hype and confusion, the underlying potential is real – and is beginning to be realised". Indeed, various countries in the Asian continent like China and private enterprises have invested heavily in cloud computing, and China showed exceptional promise in this area. The statistics of 2017 released by the United Nations, with approximately 1.4 billion people, showed China has the biggest population in the world. All of the citizens expect quality of service, specifically to access government services, which can be achieved through ICT. Chinese government's 2011-2015-year development plan specified cloud computing as one of its main strategic investment areas, including the technology and infrastructure required to support it (Wai-Ming et al 2013). To ensure that the country keeps on improving cloud computing, cloud computing research and development centres have been established in several locations around China.

Ning et al (2015) state that cloud computing in China started late, but it has been developing quickly since then. This accelerated growth can be associated with the findings of Yue, Xinhua and Lei (2013) that revealed that the number of internet and mobile users in China ranks first all over the world. The UN Global E-Government Survey (2012) attributed this rise partly motivated to preparation for Olympic Games and World Trade Organisation (WTO); however, the rise kept accelerating. Arguably, Shen et al (2012) indicate that the United States of America owns many cloud computing companies, but China owns the largest number of ICT consumers in the world. Zhang et al (2014) point out that ever since China shifted from an isolated centrally controlled economy to the open-market economy in the global economy, administrative reformation on central and local government institutions started to adapt the economic system. During the course of this transformation, the penetration of ICT and the development brought dramatic changes to organisations and individuals on various respects in the Chinese governmental context. According to UN Global E-Government Survey (2012), the Chinese government has long been striving to promote the use of ICT and was rewarded with continuously rising ranking in the global chart of e-government application. Like any developing country, China took steps to use ICT, particularly e-government, as a tool to

modernise working conditions that have positively impacted service providers (government) and recipients (citizens) (Wang & Zeng 2009).

Followed by considering that traditional archiving cannot assist with mass data, China decided to digitise traditional data such as business contracts, government's official documents and others into digital records (Aas & Kärberg 2010). This was influenced by eagerly seeking solutions for improvement of the efficiency of interactions with government. To date, An et al (2017) point out that most of the local governments, following the national government, have developed their own digital archive bureaus. These authors also indicate that digital archives in the Chinese bureau in the domain of e-government involve various medium formats, such as videos, audio and scanned documents. The governmental documents are the most important production of the Chinese government, which contain most of the information of government affairs. The Chinese government and the State Archives Bureau emphasised that filing and long-term preservation of electronic records in e-government activities should be prioritised when archiving is conducted (Qiuhui 2010). This is in cognisance of the fact that one of the basic functions of an electronic records centre is to receive and preserve the current electronic records formed in e-government activities and to provide information for all kinds of government activities and policies. Qiuhui (2010) observes that Chinese archives have been divided into comprehensive, department and enterprise archives. Comprehensive archives are considered the richest collection and serve the whole society owing to the fact that it contains the prominent sociality. Department archive serves special functions for the departments. It is popular for its service scope, which is comparatively narrow, and industrial and special features are distinctive, prominently covering storage and use of special archival materials that involve technological archives. Just like artificial intelligence, cloud storage and e-government liberate people from paper-based labour and enrich human intellect and creativity. However, the public sector is sceptical of having its records in the unknown storage.

2.4.3.3 Cloud computing and e-government in Africa

The United Nations Department of Economic and Social Affairs (UNDESA) (2016) points out that African countries have been implementing digital records and e-government services in their respective countries, but are lagging behind the European countries. This is evident in the findings that revealed that all African countries are in the lower two tiers of the E-government

Development Index (EGDI) (the low EGDI and middle-EGDI categories). The top performers of e-government with high EGDI values in Africa are Mauritius, ranked globally at 58th, Tunisia at 72nd, South Africa at 76th, Morocco at 85th, and Seychelles at 86th. According to the United Nations (2014), the EGDI is a "composite measure of three important dimensions of e-government, namely: provision of online services, telecommunications connectivity and human capacity." It ranks progress of countries on e-government based on online services advancements, best practices in e-government, ICT infrastructure and human capacity. As indicated in paragraph 1.1, e-government is viewed as a better way of enabling citizens to access public services in a most convenient, transparent and cost-effective ways. Chipeta (2018) further suggests that e-government has the potential to promote Open Government Data (OGD) in Africa.

For example, in Kenya variety of developments took place pertaining to records management in general that are worth noting and which reflect on the initiatives around the management of electronic records (Ambira 2016). Furthermore, the survey of 2014 revealed that Kenya ranked among the top 20 countries on e-government in Africa at position nine. It stood at position 119 globally out of 193 countries ranked (United Nations 2014). As a sign of progress in digital storage, the Kenyan government approved the use of electronic signatures in their transactions, which also indicates that e-government is on course. This clearly indicates that there is a need to manage electronic records in order to ensure their authenticity, secure and reliable records as a basis for efficient and effective service delivery. Despite the positive progress, Wanjiku (2009) argues that nowhere does capturing or managing authentic or reliable electronic records reflect. Such prominent absence indicates that there is no legislation that provides the use of cloud or digital storage. The lack of legislation leads to disconnection across the government departments from working collectively towards delivering services to the citizens (Ambira 2016). However, Mwangi (2012) points out that following the efficiency of online services, the Kenya National Archives and Documentation service embarked on the digitalisation of selected archival materials in 2007 primarily to facilitate access to its archival holdings the Kenyan citizens and other researchers. Ambira (2016) notes that this was done on materials that were heavily used and those that were physically deteriorating. The hindrances of implementing e-government services in African countries are similar, where IT infrastructure is the major problem.

2.4.4 Perception of public sector about cloud storage

AlZain, Pardede, Soh and Thom (2012) suggest that cloud computing increased rapidly in many organisations influenced by fast access to information and considering the reduction of IT infrastructure costs it saved. Shuijing (2014) notes that cloud paradigm includes data preservation, high levels of expertise on the part of CSP, scalability, affordability and availability. The author postulates that so far, some studies showed that many organisations that have adopted SaaS have enjoyed a return on investment of around 600%. Despite the empirical evidence that shows the benefits of cloud storage, the public sector prefers paper-based to digital formats. In the same breath, Shuijing (2014) contends that the consumers' loss of control over data is a disadvantage. The study established that the customers are concerned that they are not in control of their information. What mostly worried them was the issue that their data are entrusted to the CSP who in turn moves it from one third party to the other, which is unclear how modern laws might apply. Dahiru et al (2014) note that unexpected losses of data constitute another major fear perceived when applying cloud adoption. According to the authors, the records managers also expressed more concern about the mismanagement of data by individuals/personnel responsible for managing the data locally. Looking through the lens of the DCC Lifecycle model, an interaction can be observed between preservation action and store towards enforcing security, privacy and trust. It is believed that the advent of cloud, just like telephone and electronic mail, has enabled another channel for business to get done. Contrary to electronic mail and the telephone, it is not easy for consumers to identify the persons that are handling the cloud. Stuart and Bromage (2010) opine that the widespread access of cloud, which normally is in the web suggests that it is not helpful to know the person you are dealing with or is dealing with your information. For instance, people prefer to use private cloud-hosted electronic mails or private storage to send or receive or store confidential information. This tells that trust is a key element when using the cloud.

Cloud computing provides enormous advantages in data storage and access where benefits outnumber the weaknesses (Anand, Ryoo & Kim 2015). Lately, cloud-based services have become prominent in relation to on-demand services and unlimited storages in the organisations (Moghaddam, Ahmadi, Sarvari, Eslami & Golkar 2015). The elasticity of cloud storage ensures that space is not what the consumer can be concerned about. Shuijing (2014) postulates that contrary to the traditional way of record keeping, cloud computing provides data preservation, a high level of expertise on the part of CSP, scalability, affordability and

availability. The author adds that while the users are guaranteed access to their data anywhere at any time, CSP get the benefit of control over content, set access terms as well as monitoring usage statistics. Additionally, copyright holders are protected by the CSP with an additional security from infringement.

De Lange, Von Solms and Gerber (2016) opine that the success of the organisation is reliant on information being readily available and the integrity of this information being reliable, and the confidentiality of such information being assured. Pederit and Mainoti (2016) observe that cloud storage has proved to be a viable model for delivering IT services through the web. It became a solution and service to users by providing the ability to share distributed resources stored by a central CSP at minimal setup costs. These resources can be virtually shared regardless of geographic locations. In addition, authorised officials are not restricted to one place in order to access data as currently practised in the various government departments due to fear of adopting technology that simplifies ways of providing improved services.

In support, Kumar, Sehgal, Chauhan, Gupta and Diwakar (2011) state that the advent of cloud computing, whose adoption has steadily increased in many companies, its opportunities must be given attention. As opposed to the current practice used by various organisations for records management, Lu and Ramamurthy (2011) believe that the growth of cloud computing has made it a viable alternative compared to the existing IT infrastructure that exists within the organisation's LAN. Various organisations manage their IT infrastructure (LAN); however, data storage and remote access are not efficient or effective due to minimal access. Low, Chen and Lu (2011) maintain that cloud computing is a global option and investment. While the organisations get an opportunity to concentrate on other strategic matters, the third party in the cloud cares for data. Dahiru et al (2014) suggest that it contributes to creating access to computer resources for enterprises in developing countries where the possibilities of doing so are challenging. The adoption of cloud storage should not be avoided by the public sector that envisions improved e-government services in favour of holding on to the traditional way of paper-based record keeping.

2.4.5 Risks and vulnerabilities associated with cloud computing

Despite the advantages in the business perspective, cloud computing also presents challenges, particularly regarding the distrust of users to put their data on computers that do not have

control (Mirashe & Kalyankar 2010). Data security is potentially catastrophic for various types of cloud computing services. The authors also point out that several organisations have been working to develop specific safety standards for cloud computing, taking these surveys in a large number of areas, including auditing, applications, encryption, governance, network security, risk management, and storage virtualisation. The findings of Dahiru et al (2014) argued that security, privacy and trust issues have been major concerns even before the introduction of cloud computing and play a major role in the decision to adopt SaaS cloud-hosted applications. The research findings of De and Pal (2014) revealed that security is the most important technical factor that obviates cloud adoption. According to Julisch and Hall (2010), several studies showed that security, privacy and trust are critical issues that can inhibit the adoption of cloud computing. Dahiru et al (2014) assert that security is about the vulnerability of data in the cloud and the fear of attacks by third parties while privacy is about breach of trust by the CSP of official or personal information. Vulnerabilities are deemed security-related errors that cause weakening or removing of resistance to the environment. Attackers exploit vulnerabilities using techniques according to their ability (Grobauer, Walloschek & Stocker 2011). It is guaranteed that the responsibility for security in the case of cloud storage lies with the CSP.

Ebaid (2011:108) observes that it is difficult for organisations to avoid risks. However, Ngoepe (2012) contends that what matters most are the identification and management of risks that the organisation is exposed to. Schellnack-Kelly (2013) notes that migration of digital information in open and accessible formats may result in the original structures of the information sources being lost. This is regardless of whether data are virtually or manually stored and accessed. In stark contrast, despite the considerable benefits offered by cloud storage, Kong and Lei (2016) argue that there are some serious concerns that have affected the reliability and efficiency of modern and ongoing concepts. Ngoepe (2014) mentions that both public and private organisations face different kinds of risks that affect the reliability of records and effectiveness of internal controls on a daily basis, such as losses, negative cash flows and ultimately, bankruptcy, which can lead to liquidation. Like any company, the CSPs are not immune to bankruptcy and they cease their operations or are acquired by other companies, which eventually leads to inaccessibility and loss of records. Indeed, information security is a crucial component in the success of any organisation, regardless of what environment the organisation functions in.

De and Pal (2014) contend that despite the hype surrounding the cloud, enterprise customers, including some government departments, are reluctant to deploy their data to cloud storage. On the other hand, Brender and Markov (2013) argue that in some environments, organisational culture is a major obstacle towards adopting cloud computing as well as organisational awareness of regulatory compliance, data location, security and privacy. Some organisations are very sensitive that what they have should not be seen anyone due to the nature of sensitivity. Low et al (2011) hold that with the advent of cloud computing, organisations face the question of whether to outsource their data to the imaginary cloud storage. De and Pal (2014) note that when data are outsourced to the cloud storage, the client confers a certain degree of trust to the CSP to take proper security measures in order to protect it from external and internal attacks. Often, the question comes with security, which is one of the major issues that reduce buy-in by the cloud consumers because data privacy and data security continue to plague the market.

Furthermore, like any organisation, the government departments of South Africa possess various types of data that contain a wide range of sensitivity that can be catastrophic should it land in the wrong hands. Other research findings showed the concerns about loss of control over data, trustworthiness of CSP, data confidentiality, software vulnerabilities, legal issues about data location as well as data privacy (Rocha & Correia 2011). Shuijing (2015) states that risks of data security are compounded by the open nature of cloud computing. Such challenges have prompted scholars to identify and find solutions. That is attributed to security, which is frequently cited as a significant concern for those considering to use cloud storage, particularly for sensitive, commercial, or personally identifiable information whereby security concerns range from CSP, infrastructure and end-user (public sector). According to Ryan (2013), some of the scepticisms raised by the public sector to entrust data to the third party are:

- Cloud storage is a shared resource where other users cannot be guaranteed to be not harmful because legitimacy of fellow users is not guaranteed.
- In the event that security mechanisms lose grip, illegal users can modify or delete data in the cloud.
- Data should be accessible regardless of location, but with minimal extent.

According to Duranti and Jansen (2013), there is a myriad of risks and challenges that every organisation should heed. Arguably, with a system that provides improved accessibility and opens up the platform to multi-node access, one must take into account the risks associated

with improvement. Gonzalez et al (2011) observes that security is contentiously regarded a major requirement for cloud computing. Cloud storage offers good services to the users, but security remains a major threat, it is inevitable that CSP address information security. According to De Lange et al (2016), the purpose of information security predominantly aims to preserve the confidentiality, integrity and availability of information. However, many organisations are worried about their users' data that have been stolen and used for other purposes, which can be associated with breaching of confidentiality. Gerber, Von Solms and Overbeek (2001) define confidentiality as the property that information is not made available or disclosed to unauthorized individuals, entities, or processes. Ramgovind, Eloff and Smith (2010) advise that in order to provide a secure cloud computing solution, it is essential to decide on the type of cloud to be implemented between the deployment models, for example, public, private and hybrid, and this role should be conducted by the IT managers or security officers. Kulkarni et al (2012) argue that cloud computing is made vulnerable because it runs on a networking infrastructure; and that leaves it open to attacks. These authors also point out that if implementing adequate controls does not properly safeguard information, the impact of both short- and long-term information security breaches can have a devastating effect on an organisation – and can even threaten the survival of an organisation. Gibson et al (2012) lists the following as the common concerns of cloud computing: security, privacy and data availability.

Safa et al (2015) further indicate that it is widely accepted that both technological controls and human behaviour are central aspects that need to be addressed when protecting information. According to Cachin, Haas and Vukolic (2010), the threat was confirmed by the survey conducted by the IDC, which revealed that the primary challenge of 74% of CIOs in relation to cloud computing is security. It was assumed that the combination of those two factors makes the government departments opt to rather keep data in their own premises. However, such move restricts them from functioning effectively bearing in mind that they need physical location to access that data.

Gonzalez, Kaplan, Saltzman, Winkelman and Woods (2017) observe that the security status of cloud services is reliant on the factors such as security application running on the system, the hypervisor and associated protection measures, the design patterns used to isolate the control plane from cloud tenants as well as protection given by the CSP. The authors also listed the following attacks that are experienced on cloud computing:

- Outside or inside attack: it exports weakness in cloud access control mechanisms that are on firewalls of the CSP.
- The theft of valid credentials of a cloud user at some location outside the cloud.
- Attacker using valid credentials and prior legitimate access to the cloud.

The proliferation of cloud computing has motivated malicious people to revise attack techniques in order to cope with the newly introduced features of cloud computing infrastructures (Hamdi 2012).

2.5 The view of public sector on digital preservation in the cloud

According to Nam (2012) and Adu et al (2016), the global perspective on digital revolution is one that has received popular approval for the information from professionals, scholars and practitioners for influencing the way in which information is gathered, managed, processed, stored and accessed. The Canadian government (2012) espouses that various governments that started with paper-based storage of data have supported the shift to digital preservation through enacting a number of legislations and changes in policies. Supported by the findings of Pappel, Pappel and Saarmann (2012), the Estonian paperless records management as part of e-government has been set as an example in Europe on numerous occasions. Indeed, in an attempt to catch up with the continuous development of technology in the world, South Africa enacted various laws and endorsed ISOs that support the envisioned e-government services. Adu et al (2016) contend that the implementation of e-government could not be complete without the ancillary process of records maintenance because the information generated by the government deserves to be preserved for the general public to access.

Tsan-sheng et al (2014) explain that having learnt the way the public sector keeps its records it is clear digital preservation is relevant mainly due to the number of digital documents that need to be preserved for long periods of time has increased significantly over the past years. While the public sector performs its activities and takes decisions, there is a need to preserve informative and evidential value from the point of view of transparency (Pappel et al 2012). Given that the amount of content available is growing constantly, it is essential to avoid absence or loss of vital information. The capability to preserve information is a necessary condition to make a cultural heritage available for the posterity. In the same breath, Rogers (2015) opines

that the internal support for accountability depends on how information and records are created in the first place, and how they are managed, and preserved in order to provide for government accountability. One of the critical aspects of government records is the ability to attest to their authenticity over time and across space.

Digital preservation gave an assurance to the right to information law that the government would accumulate and maintain information that is authentic, verifiable and reliable (Adu 2015). The right to information forms a bedrock of the Constitution of the Republic of South Africa. Section 32(1)(a) of the Constitution provides that everyone has a right of access to any information held by the state. As indicated in paragraph 2.3, Section 32(32) of the Constitution stipulates the enactment of the national legislation to give effect to the fundamental right to information. In the same vein, ICA also provides that the public has the right of access to archives of public bodies wherein both public and private entities should open their archives to the greatest extent possible. This is informed by that access to archives of government is essential for an informed society. ICA further assert that public and private institutions holding private archives do not have a legal obligation to open the private archives to the external users unless specific requirement or regulation imposes responsibility to them. The Promotion of Access to Information Act (PAIA) 2 of 2000 is the national legislation contemplated in section 32(2) of the Constitution. PAIA gives effect to the constitutional right of access to any information held by the state and any information that is held by another person and that is required to for the exercise or protection of any rights, and to provide for the matters connected therewith. Section 9 of PAIA also recognises that the right to information is subject to certain justifiable limitations aimed at, amongst others: (a) the reasonable protection of privacy, (b) commercial confidentiality as well as (c) effective, efficient and good governance. However, Rogers (2015) opines that one of the key aspects of government records is the ability to attest to their authenticity overtime and across space. The integrity of government records must not be compromised. In that regard, Adu et al (2016) point out that the preservation of records provides an appropriate policy for the enactment of the law that creates a technical infrastructure in order to give life to the right to information law. Considerably, Adu (2015) asserts that the exercising of one's right to request for records hinges on the availability of information about records in the government. International Records Management Trust (IRMT) (2011) revealed that the right to information law fails if records cannot be identified, retrieved and used, if their integrity cannot be established and properly stored. With the quest to implement cloud storage, creating the infrastructure for the preservation of digital records

cannot be treated in isolation and exclusive to the application of the right to the information law. The two concepts are intertwined and operate hand in hand. Alexander (2014) and Mizrahi and Marcos (2014) share a similar view that records managers in the United Kingdom and the United States of America collaborate with the right to information oversight bodies to harmonise record-keeping policies across the public sector.

The Institute of Directors Southern Africa (IODSA) points out that technology governance and security have become significant in the technology spheres Technology has gone beyond the level of an enabler of the organisation, it has become both the source of an organisation's future opportunities and of potential disruption, an excellent example of how risk and opportunity are increasingly two sides of the same. IODSA adds that the security of information systems has also become critical. This is one other reason the General Information Technology Controls, (GITC) 2018 indicate that the controls should be utilized in the cloud and e-government services. According to IODSA and Deloitte, ITGC are controls that apply to all systems, components, processes and data for a given organization or IT environment. GITC provide the foundation for reliance on data, reports, automated controls and other system functionality underlying business processes. This would enhance authenticity and reliability of records.

2.5.1 Opportunities of digital preservation

According to Ferreira et al (2017), digital preservation ensures that the content in digital format remains accessible over time, reliable and authentic. Tzitzikas, Kargakis and Marketakis (2014) argue that digital preservation is not only against loss or corruption, but also against hardware/software technology changes, plus changes in the knowledge of the community. It is every organisation's concern to have its footprints in the form of records that are continuously available to the posterity in order to have referral and evidence. There is a need for services that help archivists to check that the archived digital artefacts remain intelligible and functional, and in identifying the consequences of probable losses (obsolescence risks) (Tzitzikas et al 2014). Delaney and De Jong (2015) observe that digital preservation comprise the digital lifecycle management processes, spans and archive operations that consist of acquisition, ingest, metadata creation, storage, preservation management and access. This view has similarities to Higgins's (2008:136) DCC Lifecycle model, which is composed of store, access, ingest, create, and receive and migrate. Higgins (2008) and Delaney and De Jong (2015) share similar views by indicating that digital preservation applies to both born digital and reformatted

content. This means that based on the origin of data, it must also be accessible when needed. To prove the reliability of data, digital preservation has the following key concepts: integrity and authenticity. Accordingly, Sierman (2012) points out that a repository must be able to provide evidence that a particular object under digital preservation control is what it purports to be (authenticity) and that it has not been corrupted over time (integrity). In the event that changes have been made on digital data, documentation must be made detectible and manageable (Delaney & De Jong 2015). These authors further state that the digital policy document on the organisation's commitment to preserve digital content for future use, specifically file formats to be preserved, and the level of preservation to be provided, ensure compliance with standard and best practices for responsible stewardship of digital information. Ngoepe (2010) and Viana and Sato (2014) contend that in the context of long-term preservation, most of the information that needs retention is reference data, which normally changes little once it has been recorded. In a normal situation, two possible applications for long-term preservation is the preservation of data for legal auditing and administration.

2.5.2 Challenges of digital preservation of archives

Barateiro, Draws, Neumann and Strodl (2012) hold that digital preservation aims to ensure operability and usability of digital information. However, the benefits offered by long-term preservation raise challenges with software, hardware and maintenance. While organisations need to store and preserve different forms of digital data for long periods, the preservation of document integrity over longer periods is a daunting task that various organisations, including the public sector, struggle with, both technically and organisationally. Changes of technology (new formats or standards), changes of environment (new legal obligations) as well as the disappearance of services need to be addressed for ensuring usability in the long run. Accordingly, Barateiro et al (2012) contend that changes in the environment technology services and data potentially have immediate effects on the system's functionality. Almeida, Cendón and Souza (2012) view that the longevity of digital data is affected both by technical changes and technical progress.

Yu (2010) listed the following concerns of digital preservation: contextualise, access, control, accountability, display and persuasion. In many instances, the digital obsolescence might be caused by the ongoing development of new software and new formats, so the risk of obsolescence can be estimated from a global environment. Extensively, Barateiro et al (2012)

note that threats might emanate from humans, hardware/software faults, large-scale disasters and institutions. The authors explained the following threats:

- Human-related threats: while employees can unintentionally or intentionally erase or overwrite data, operators can lose media support or store data inappropriately.
- Hardware/software-related threats: hardware components may fail temporarily or permanently. Bugs may affect software and the support can be discontinued. Hardware systems can become obsolete. This implies that it may be extremely difficult to make a given system communicate with others. Storage media readers and writers can become obsolete as well as the media supports employed. Storage media are not completely reliable over a long period of time.
- Environmental dependent threats: natural disasters or conflicts can pose dramatic threats to archival sites.
- Institutional dependent threats: the organisations that have data to be preserved but whose main activity is not data preservation have to face a complex budget planning for maintaining their archives, and in most cases the budget allocation is very limited. Moreover, institutions can change goals over time or they can go bankrupt. This poses a serious threat to the storage systems, which can be lost, damaged, left without documentations, and so forth.

According to Almeida et al (2012), the issue of digital preservation presents itself as a real problem to be solved by the institutions, especially those that have a legal obligation to maintain long-term documents. Issues of authenticity and integrity, preservation lifecycle of assets as well as attention to the interests of particular communities of practice, such as archivists, have major areas of interest for the DCC Lifecycle model. Nguyen and Lake (2011) share that a complicating aspect of digital preservation is the heterogeneity of data. The data comes from a slew of specialised domains, with diverse application software running on a variety of platforms. The manifestation and representation of the data can be in formats as different as Microsoft Office documents, relational database files, geospatial images, or multimedia materials.

Currently, no one choice is right for all government departments, because of circumstances that change over time and rules used in various environments. Given that South Africa has adopted the international standard of archiving, the ISO 14721:2012, Reference Model for Open

Archival Information Systems (OAIS) is applicable to archiving and should be of value to organisations responsible for making information available for a longer term. However, ISO 14721:2012 again argues that 'long-term' does not imply that the OAIS is permanent, it only means that the archive has the responsibility for storing information "long enough to be accessed with impacts of changing technology, including support for new media and data format" (Beagrie & Jones 2001). According to Barateiro et al (2012), the issues of digital preservation are addressed by maintenance activities, resulting in a very expensive adaptation or effort of replacement. However, that is not the responsibility of the client, but of the CSP.

2.6 Disposal of digital records in the cloud

The DCC Lifecycle model reflects that the disposal of records forms a crucial part of records management. Disposal can be in the form of transferring records to archives or destroying the record. Constantopoulos et al (2009) suggest that, typically, records might be transferred to another archive, repository, data centre or custodian. In other instances, records are destroyed. The record's nature may, for legal reasons, necessitate secure destruction. The ICA (2005) defines 'record' as recorded information produced or received in the initiation, conduct or completion of an institutional or individual activity and that comprises content, context and structure sufficient to provide evidence of the activity. This is applicable regardless of medium and format of a record. The International Standard of Records Management (ISO 15489-1) stipulates that records must be characterised by authenticity, reliability, integrity and usability in order to meet the business needs and for accountability purposes over time. Records are essential in the life cycle of records management up to the disposal of records for long-term curation and preservation in accordance with documented policies, guidance or legal requirements (Higgins 2008; Constantopoulos et al 2009).

However, the NARSA Act stipulates that disposal can only be performed after obtaining disposal authority from the national archivist. This is evident in the findings that revealed that all African countries are in the lower two tiers of the E-government Development Index (EGDI) (the low EGDI and middle-EGDI categories). The top performers of e-government with high EGDI values in Africa are Mauritius, ranked globally at 58th, Tunisia at 72nd, South Africa at 76th, Morocco at 85th, and Seychelles at 86th. According to the United Nations (2014), the EGDI is a "composite measure of three important dimensions of e-government, namely: provision of online services, telecommunications connectivity and human capacity." It ranks

progress of countries on e-government based on online services advancements, best practices in e-government, ICT infrastructure and human capacity. As indicated in paragraph 1.1, e-government is viewed as a better way of enabling citizens to access public services in a most convenient, transparent and cost-effective ways. Chipeta (2018) further suggests that e-government has the potential to promote Open Government Data (OGD) in Africa.

Having indicated what legislation clarified on the disposal of records, it is ostensibly clear that the disposal was based on the in-house records management. This is informed by that currently, records are stored on the government premises and not in the cloud and this practice is in line with NARSA Act of 1996. Either the paper or digital records are disposed manually on government premises preceded by the approval of the national archivist as prescribed in the Act of 1996. Cloud storage is a multi-tenancy model that is economically attractive to different cloud consumers who share the space. This creates technical difficulty when records are supposed to be disposed of in the form of destruction. Duranti and Jansen (2013) argue that the multi-tenancy model utilised by cloud service providers to reduce service costs adds additional complications with regard to the ultimate destruction of records. The authors also opine that the traditional method of wiping a disc and overwriting the sectors with random digits cannot be accomplished when other tenants are concurrently maintaining active records on the same disc. Any attempt to destroy the disc can unintentionally have a negative effect on the records of other clients. On the one hand, the National Archives Records Act indicates that records that are not destroyed are preserved for a lifetime or 400 years.

Roper and Millar (1999) observe that the concept of archives' lifecycle utilises the analogy of biological organisms constituting the following three stages: current (active records), semi-current (semi-active records) and non-current records (inactive records or archives). According to Mnjama (1996:24) and Mnjama and Wamukoya (2006), in the creation stage, the current or active information sources are created and maintained for the objectives of administrative, executive, financial and legislative activities. The DCC Lifecycle model sees the lifespan of a record as a progression through distinct stages from creation to disposal. Ngoepe (2012) suggests that record management, as a process of managing records from their inception to their disposal (lifecycle), exists as a key enabler for organisations to account for their actions. If it is properly conducted, it ensures that organisations retain records for as long as they are required and, when no longer needed, they are destroyed appropriately or disposed of in various ways like transferring to archive services. Typically, data might be transferred to another

archive, repository, data centre or custodian (Higgins 2008). The data's nature may, for legal reasons, necessitate secure destruction. For non-archival records that are required for lawsuit, PAIA indicates that such actions might not be disposed in the form of destruction until the Manager: Legal Services has directed that the hold on destruction can be lifted.

Franks (2013) states that the primary purpose of records retention and disposition is to ensure that records are retained only for as long as necessary and then disposed of when they no longer have value. However, Lwonga, Ngulube and Stilwell (2011:4) maintain that in most governmental bodies in sub-Saharan Africa, too many records are kept for too long due to a lack of disposal authority. Ngoepe (2012) further upholds that as outlined in the King III report, every institution should have an information committee of senior executives who audits the information processes and monitors the full lifecycle of information – from creation or receipt to disposal. This ensures that the organisations become more accountable for the way in which they dispose of their records. While in some instances data are destroyed to safeguard the disposal function as part of lifecycle of records, organisations need to be in a position to explain the absence of records that were once held. According to NARSSA 1996, paper-based archival records shall be kept safely in general registry until they are due to be transferred to the national archives repository. Franks (2013) notes that transfer procedures should be conducted as prescribed by the National Archives in the Records Management Policy Manual. To determine records retention requirements, records are appraised based on their current operational, regulatory, legal, fiscal, and historical value and legal research is conducted to identify governing laws and regulations. On the other hand, the National Archivist determines the activities with regard to public records where no public records (including e-mail) will be destroyed, erased or otherwise disposed of without prior written authorisation from this official. Hare and McLeod (1997:32) reveal that retention schedules are essential towards meeting acceptable records management standards. The retention schedule helps to:

- provide standards and consistency across the organisation on records management issues
- identify unnecessary duplication, encourage timely relocation of material from costly office space to less expensive office space
- promote effective management and identify records of long-term value as early as possible

- secure records from accidental destruction and plan for their preservation (Hare & McLeod 1997).

2.6.1 Significance of records disposal from cloud storage

Having indicated that the South African records are mainly in the formats of paper, audio and film, this section discusses the significance of data disposal from cloud storage. Contrary to paper-based processes in the current records management environment, the cloud storage allows public sector officials to conduct their disposal function in an automated manner. According to Higgins (2008), disposal of data, as depicted on the DCC Lifecycle model, takes place when data, which has not been selected for long-term curation and preservation in accordance with documented policies, guidance or legal requirements. Considering that the disposal aspect of data requires hardware and software, Almeida et al (2012) suggest that sometimes the length of the required availability of data exceeds the lifespan of various electronic formats and cryptographic mechanisms used to store and preserve authenticity of data and its legal validity. Knowing that cloud storage is the property of the CSP, it is up to the client to decide on options that suit the organisation. In the process, prescription fees vary per gigabyte and model selected. Higgins (2008) outlines the following benefits of disposal process:

- Avoiding unnecessary storage costs incurred by using office or server space to maintain records no longer needed by the organisation.
- Supporting compliance with the fifth data protection principle if records contain personal information (this principle requires organisations not to keep personal information for longer than necessary).
- Finding and retrieving information are quicker and easier because there is less to search.

2.6.2 Risks of failing to dispose data

As depicted in the DCC Lifecycle model, disposal forms part of records' lifecycle. The NARSSA indicates that records that are no longer required must be destroyed; however, there should be evidence that such record existed. Rightly so, in the digital space where organisations are charged according to what they have stored with the CSP, it gives them an opportunity to

open new space. Currently, like in the case of the South African government departments, destruction of paper records is carried out in a variety of ways, including shredding, pulping and burning. NARSSA points out that burying records or putting them on a rubbish tip, are not acceptable methods of destruction because they remain accessible to anyone who finds them. Records should be destroyed with the level of security required by the confidentiality of their contents. In contrast, deletion of digital records from the hard disc is insufficient. In the event where an external contractor is being used for the destruction of the records, it should be ensured that the contract specifies clearly what is required, including transmission of records off site and what constitutes destruction. To uphold correct procedures as prescribed by NARSSA, the premises of contractors must be inspected both before the contract is awarded and periodically thereafter, to ensure security is adequate and that records are destroyed soon after they are received, which is a challenge to expedite the disposal process. This is particularly important if the records are confidential in any way. The contractor should be required to supply a certificate of destruction and, for confidential records, a certificate of confidential destruction.

This is influenced by the fact that the records may no longer be visible, but they are not beyond any possible recovery. The extreme measures of full destruction that are needed include overwriting with random digital code enough times to eliminate the data. Disposal schedules can be created in any medium or format but it is probably best to create and maintain them in a database, especially if there is more information about the records than disposal details. According to NARSSA, it is the responsibility of National Archivist to ensure that records are assessed to see whether they can be destroyed immediately, should be retained for a further period or has archival value and should be designated for permanent preservation. The NARSSA disposal decisions should be made in consultation with the relevant business unit and, if appropriate, legal advisors. Failure to dispose of data leaves the organisation with unwanted data despite the fact that cloud storage is elastic.

2.7 Framework for the digital management of records in the cloud

The preceding discussions have shown that policies for data storage in government departments are informed by NARSSA. South Africa has endorsed international standards in order to avoid being left out as far as transparency to information is concerned. Indeed, South Africa has legislation that promote not only access to physical information, but also to electronic records. It is also crucial to have a framework that is complemented by the regulatory framework of the

country. It discusses how data can be migrated from the current decentralised storage to digital preservation hosted in the cloud. Oyewole (2012:3) observes that shifting from primarily paper-based to digital information environments requires adequate financial, infrastructural and human capital as well as regulatory, administrative and systematic capacities. South Africa has what it takes for such migration because legislations have been enacted and international standards have been endorsed in order to support and protect the adjustment to the evolution of technology where long-lasting storage of information is enhanced (Mogale 2007). Upon digitalisation, the envisaged e-government services would be achievable. Supported by Schellnack-Kelly (2012:170), there is a need to improve the provision of accurate, accessible information to empower and facilitate better, effective service delivery to ordinary citizens.

2.7 Related studies

This section discusses various studies that are related to this study in order to look at how those studies were conducted by other scholars. These local and international studies are discussing the digitisation and storage of records in the cloud. The main focus is based on approaches employed, methods applied, types of instruments used to collect data and the findings reached. The review of these studies is intended to justify and support the methodologies used to conduct the current study as reflected in Chapter Three.

Nyide (2014) conducted a literature review on digitisation of theses and dissertations in the University of KwaZulu/Natal. These materials were intended for usage in the library of the university. Amongst the key issues to mention is that this study was concentrated to digitising the academic products such as theses and dissertations and the DCC Lifecycle model was one of the crucial frameworks that played a significant role in this study. This study used concurrent triangulation method where two methods of interviews and questionnaires were simultaneously employed. It is worth noting that the results of this quantitative study indicated that there were existing strategies however, the digitisation strategy and policies guiding the project of digitisation in the library did not exist.

Ambira (2018) conducted a study titled a framework for management of electronic records in support of e-government in Kenya. This study interpretive research para was concerned with management of electronic records as they exist within the e-government platforms and not general electronic records management. This interpretive research paradigm employed

qualitative research methodology using phenomenological design. It adopted the use of electronic records as opposed to digital records, even though e-government is anchored on digital records. It established that the general status of management of electronic records in government ministries of Kenya is inadequately positioned to support e-government. It concludes that he practices for managing electronic records in support of e-government implementation is not adequate in Kenya.

Adu (2016) conducted a study that investigated digital preservation for electronic government in Ghana. In the study, the researcher points out that digital revolution has received approval of information professionals, scholars and practitioners. This study was guided by the multi-method design and underpinned by the triangulation of questionnaires, interviews, observation and document analysis were employed, and it examined the digital preservation of e-government in Ghana. In its findings, it reveals that the creation of databases, digital publication, emails, websites information and tweets are occasioned by the use of ICT, e-government, application of legislation as well as public policies. It also identified funding, level of security and privacy, skills training and technological obsolescence as factors that pose threats to digital preservation. Furthermore, it emerges from this study that cloud computing is the least implemented preservation strategy used to address the digital preservation challenges. It recommended ministries and agencies to address digital preservation challenges by leveraging collaborative and participatory opportunities using cloud computing.

In Australia, Stuart and Bromage (2010) explored the challenges of managing and storing records and information in the cloud. This study provides that records professionals around the world acknowledge that it is becoming clear that the web is not only changing the working behaviour, but it is also changing the way records are interpreted and organisational documentation. Regardless of where the records are created, the management of these records must be held in the realm of the cloud storage. Based on experience, observation was employed to collect data for this study. It established that as organisations are changing the way to conduct business by including web 2.0 and the cloud into their own dealings, records managers need to be aware of the risks associated with virtual environment. Another key finding indicated that the incorporation of cloud into the way organisations conduct business should not be based on a technological decisions, but should be based on a decision examining risk to information of an organisation. This study also noted that cloud is not a threat itself, but its use carry risks. It encourages Australian state's organisations to consider cloud storage.

Pan (2019) conducted a study on managing records as evidence and information in China in the context of cloud-based services. This qualitative case study explored the management of electronic records as evidence and information in Chinese enterprises to support regulatory and legal framework as well as satisfying business needs. The study revealed that the impact of cloud-based service on records management practice is limited in the two Chinese enterprises (Sino-foreign joint venture and a state-owned entity).

2.8 Summary

This chapter reviewed literature as guided by the theoretical framework and research objectives of the current study. The main actors involved legislations, digital preservation, e-government services as well as cloud storage. The chapter touched on various aspects that require consideration when digitalisation is meant to begin. It again emphasised the role that the National Archivist should play alongside IT managers when the current records management migrates to the cloud. The next chapter discusses the methodologies undertaken to conduct this study.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

The previous chapter reviewed the literature regarding the topic being studied guided by the theoretical framework and research objectives of this study. This chapter discusses the methodological process and techniques employed to attain the purpose of the current study. It recognises the target population of this study and trustworthiness of research instruments. Kothari (2004) and Maxwell (2005) opine that the research process is composed of the steps that are crucial to effectively conduct an investigation and the preferred sequencing of these steps. Alasuutari, Bickman and Brannen (2008) and Gelsne and Peshkin (1992) propound that research methodology highlights the wider field of discussions about methods as well as relationship between methods and theories. This chapter presents research paradigm, research approach, nature of research, research methods, data collection instruments and ethical consideration. Figure 3.1 below illustrates a roadmap for the research methodology of this study.

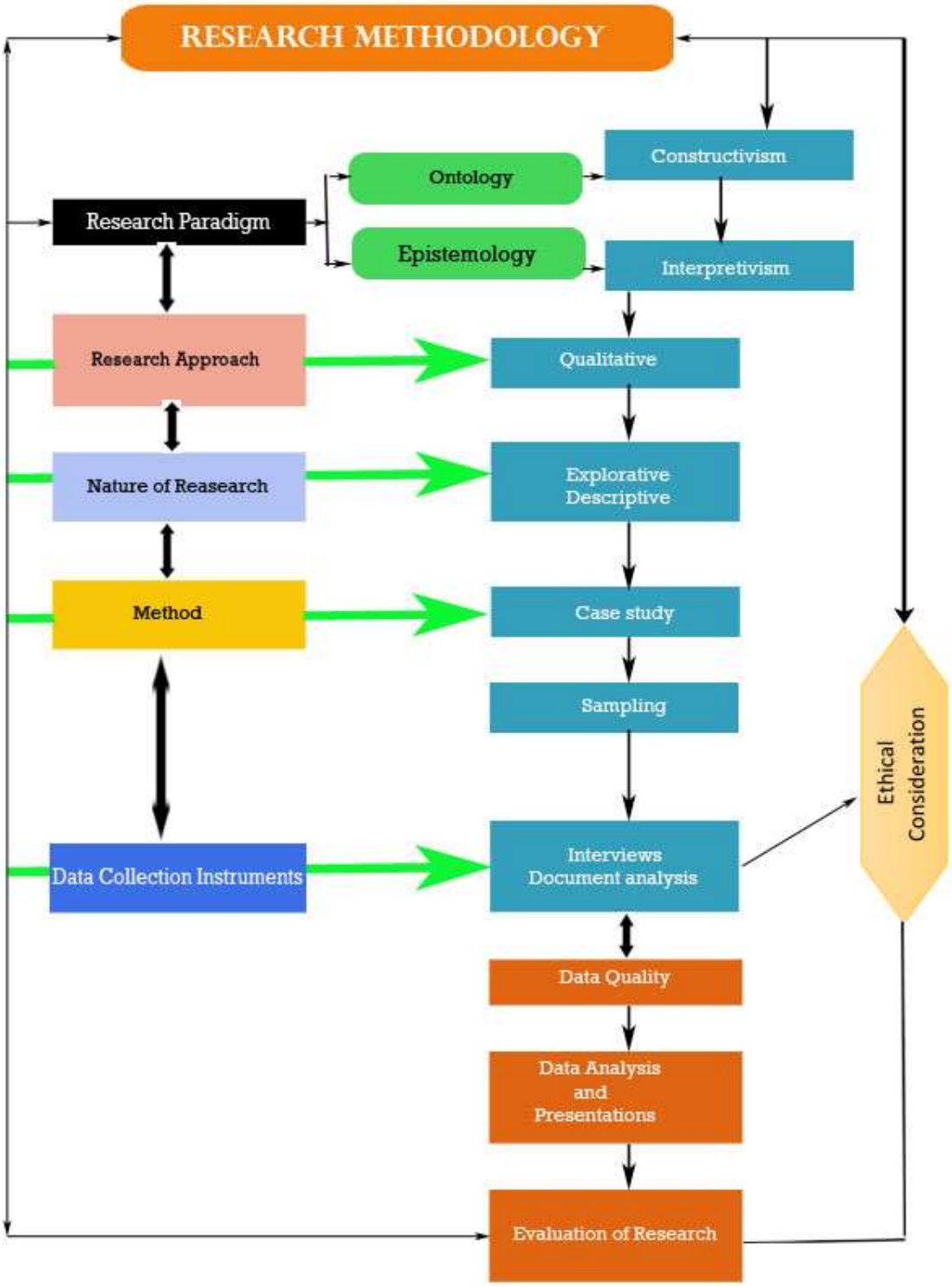

Figure 3.1 Research methodology roadmap

3.2 Research paradigm

Neuman (1997) explains that paradigm is a set of beliefs that guides the scholars in conducting a scientific study. Similarly, Bhattacherjee (2012) defines paradigm as the design and conduct of research that shape the mental mode or frames of references used to organise reasoning and observation. On the hand, Sarantakos (1993) and Mackenzie and Knipe (2006) define paradigm as a cluster of propositions that explains how the world is perceived. Furthermore, Bryman (2012) indicates that in scientific research, paradigm is defined as a patterns of beliefs and practices that regulate inquiry within a discipline by providing lenses, frames and processes through which a study is achieved. This is closely related to informing the scholars what is essential, what is legitimate, and what is reasonable. Creswell and Garrett (2008) argue that without putting forward a paradigm as an initial step in research, there would be no foundation for subsequent choices on methodology and literature. According to Leedy and Ormrod (2013) and Lysaght (2011), the contending standpoint of the research paradigm, positivism and interpretivism, which the world is dominantly centred on, are ontological (nature of reality) and epistemological (nature of knowledge) assumptions and that renders the two paradigms incompatible. Various researchers such as McMillan and Schumacher (2006), Bhattacherjee (2012:19) and Hitchcock and Hughes (1995) suggest that if researchers view the world as consisting mostly of social order (ontology) and seek to study patterns of ordered events or behaviours and believe that the best way to study such a world is using an objective approach (epistemology) that is independent of the person conducting the observation or interpretation, such as by using standardised data collection tools like surveys, they are adopting a functionalism paradigm. However, if researchers believe that the best way to study social order is through the subjective interpretation of participants involved, such as by interviewing different participants and reconciling differences among their responses using their own subjective perspectives, then they are employing an interpretivism paradigm.

Furthermore, Kumar (2005) and McNeill and Chapman (2005) state that if researchers believe that the world consists of radical change and seeks to understand or enact change using an objectivist approach, the radical structuralism paradigm is employed. Lastly, if they wish to understand social change using the subjective perspectives of the participants involved, then they are following a radical humanism paradigm. The positivist's belief is that the social world exists in the same way as the natural world, and the approach of the natural sciences could be applied to the social world (Bhattacherjee 2012:19). The author further adds that positivism

holds that science or knowledge creation should be restricted to what can be observed and measured. Positivism tends to rely exclusively on theories that can be tested directly. Such methods employ a deductive approach to research, starting with a theory and testing theoretical postulates using empirical data. Creswell (2013) views that positivists believe in the existence of absolute truth and it is associated with the quantitative research method. On the other hand, the interpretivists place emphasis on the meanings made by people as they interpret the world in a natural setting (Creswell 2012). Methods like informal interviews, inductive reasoning and observations favour the interpretivist paradigm (Creswell 2002 & Thomas 2003). Interpretive methods employ an inductive approach that starts with data and tries to derive a theory about the phenomenon of interest from the observed data (Bhattacherjee 2012). Interpretive methods, such as case study, action research and ethnography are aimed at theory building. As per the research purpose, this study aimed to source views of participants using subjectivist techniques such as interviews and ethnographic studies. Interpretivism paradigm was selected for the current study.

According to Creswell (2014b), interpretivism does not begin with a theory in mind. In interpretivism, it is believed that individuals seek an understanding of the world they live in and that leads to the development of subjective meanings of what individuals are experiencing. The goal in an interpretivist research is to get the participants' views and generate a theory and/or pattern of meanings (Creswell 2014c). Any scholar employing interpretivism relies on the feedback from the participants to construct (constructivism) ideas that will explain and support the existence of phenomena. According to Creswell (2013:8), interpretivism is aimed at producing an understating of the context of the information system and the process whereby the information systems are influenced by the context. Various scholars such as Collis and Hussey (2009:56-57) and Rubin and Babbie (2010:37) observe that the purpose of research in interpretivism is to understand and interpret daily events, experiences and social structures as well as the values people attach to these phenomena. Collins, Onwuegbuzie and Sutton (2006) argue that interpretivism is "associated with the philosophical position of idealism, and is used to group together diverse approaches, including social constructivism, phenomenology and hermeneutic approaches that reject the objectivist view that meaning resides within the world independently of consciousness". According to Myers (2013), interpretive researchers assume that access to reality (given or socially constructed) is only through social constructions such as language, consciousness, shared meanings and instruments. Myers and Newman (2007) contend that interpretivism does not regard the social world as "out there", but believes that

human beings construe it. The authors add that it seeks to investigate how humans perceive and make sense of this world, because it is people who give meaning to their social world.

In this case, where the study explores digital data on cloud storage, a researcher becomes part of the research as a meaning-maker (interviewer) interacting with other meaning-makers (interviewees). Consequently, research becomes the construction of meanings between the participants, one of whom is the researcher. Saunders, Lewis and Thornhill (2003; 2012) share the view that in order to conduct a successful interpretivist approach, it is crucial for the researcher as a social actor to appreciate differences between people. This means reality is interpreted through the meanings that people give to the life of the world. The philosophical foundations of Myers and Newman (2007) indicate that knowledge does not exist separate from the context in which it is used. Bryman and Bell (2007) observe that as opposed to positivism where results are assessed without personal value judgement, for example, reality is objective, interpretivism views reality as subjective. Rightly so, a meaning can only be discovered through language and not exclusively through the positivist paradigm (Schwandt 2007a:314-317). Interpretivism takes different ontological and epistemological positions from the positivist paradigm. Bhattacherjee (2012) listed the following unique benefits of interpretive research paradigm:

- It is well-suited for exploring hidden reasons behind complex, interrelated social processes like inter-firm relationships where quantitative evidence may be biased or difficult to obtain.
- It is useful for theory construction in areas with no or insufficient prior theory.
- It is appropriate for studying context-specific, unique, idiosyncratic events.
- It uncovers interesting and relevant research questions and issues for follow-up research.

The author also listed the challenges of interpretive research paradigm:

- It is more time- and resource-intensive when collecting data.
- It requires well-trained researchers who are capable of seeing and interpreting complex social phenomena from the perspectives of the embedded participants and reconciling the diverse perspective of these participants, without injecting biases into inferences.
- Data sources may not be reliable. Inadequate trust between researcher and participants may hinder full and honest self-representation by participants.

Having discussed the benefits and challenges, interpretive paradigm must reflect the following characteristics: naturalistic enquiry, researcher as an instrument, interpretive analysis, use of expressive language, temporal nature and hermeneutic circle (Bhattacherjee 2012).

3.3 Research approach

The most popular methodological paradigms in research are qualitative and quantitative research methods. Bhattacherjee (2012:35) highlights that quantitative and qualitative methods refer to the type of data being collected (quantitative data involve numeric scores, metrics, and so on, while qualitative research uses interviews, observations and so forth) and analysed (using quantitative techniques such as regression or qualitative techniques such as coding). Bahari (2010) observes that the main distinction between these two approaches is that qualitative is intensive while and quantitative is extensive. Creswell (2012) points out that the mixed-method is a third research approach. According to Plano-Clark (2010), it is named mixed-method research approach because it combines qualitative and quantitative approaches. It either uses the qualitative approach or supplement it with quantitative data. This happens when researchers use interviews to collect data and use questionnaires to supplement data of interviews.

Quantitative research tests objective theories by examining the relationship among variables that can be measured by the use of instruments so that numbers can be generated and analysed using statistical procedures (Creswell 2013). Leedy (1997:104) opines that it uses mathematical analysis where data or evidence is based on numbers and variables are central. According to Bless, Higson-Smith and Sithole (2013:56), quantitative method depends mainly on measurement to compare and analyse different variables. When using this method, the researchers focus on collecting data according to a set of steps and try to remain as objective and neutral as possible. This approach aims to bring relationships between variables and as a result it omits the process of interpretation that goes on in human groups (Bryman & Bell 2011). Data collection methods in quantitative research include surveys (questionnaire), content analysis that seeks to quantify content in terms of predetermined categories and experiments (Leedy 1997). According to Bhattacherjee (2012:44), quantitative data can be analysed using techniques, such as regression or structural equation modelling.

The mixed method approach, which is also called the multi-method approach, is an approach

of inquiry that combines both qualitative and quantitative methods in the same study (Leedy & Ormrod 2013). Neuman (2011) and Johnson and Onwuegbuzie (2004) define mixed method research as the class of research where the researcher mixes quantitative and qualitative research techniques, methods, approaches, concepts or language into a single study. Bhattacherjee (2012:35) notes that sometimes, joint use of qualitative and quantitative data might help generate unique insight into a complex social phenomenon that are not available from either types of data alone, and hence, mixed method designs that combine qualitative and quantitative data are often highly desirable. Gomm (2008) mentions that its purpose is to get more than one purchase on the phenomenon and to triangulate data from one approach with data from another, which gives a researcher the opportunity to view the research problem from both the quantitative and qualitative perspective. According to Creswell (2009), this research approach is useful when either the quantitative or qualitative approach by itself is inadequate to best understand a research problem or the strengths that both the quantitative and qualitative research can provide the best understanding.

These three methodological paradigms are sometimes referred to as methodologies, traditions or even designs. Cresswell (2006) opines that each of these approaches, qualitative and quantitative, has been associated with interpretivism and positivism, respectively. However, Sarantakos (2013) suggests that these methodologies are reliant on the foundations of social science which involve ontology, epistemology, methodology, designs and then also instruments of data collection. However, it is argued that quantitative research is weak in understanding the context or setting in which people talk and researchers use their personal biases and interpretations. One other major limitation is that measurements typically detach information from its original ecological real-world context. Table 3.1 discusses the three research approaches and demonstrates their strengths.

Table 3.1 Comparisons of research paradigm (Adopted from Ngoepe 2012)

Theme and paradigm	Strength	Weakness
Qualitative and interpretivism	• Data-gathering methods are seen more as natural as artificial. • Ability to look at change processes over time. • Ability to understand people's meaning. • Ability to adjust to new issues and ideas as they emerge. • Contribute to theory generation.	• Data collection can be tedious and they require more resources. • Analysis and interpretation of data may be more difficult. • Harder to control the pace, progress and end-points of research process. • Policy makers may give low credibility to results from the qualitative approach.
Quantitative and positivism	• Provide wide coverage of the range of situations. • Fast and economical. • Where statistics are aggregated from large samples, they may be of considerable relevance to policy decisions.	• The methods used tend to be rather inflexible and artificial. • They are not very effective in understanding processes or the significance that people attach to actions. • They are not very helpful in generating theories. • Because they focus on what is, or what has been recently, they make it difficult for policy makers to infer what changes and actions should take place in future.
Mixed method and pragmatism	• It combines both qualitative and quantitative to collect data.	• Numbers versus words. • Artificial versus natural.

3.3.1 Qualitative research approach

Atkinson (2002) opines that qualitative research is a social inquiry that concentrates in a way that people interpret and make sense of their experiences and the world they live in. Contrary to quantitative approach, it describes multiple realities, developing deep understanding, building theory as well as capturing everyday life. Considering that it gathers information through interviews, qualitative data is rendered open-ended. According to Leedy and Ormrod (2013), the analysis of qualitative data consists of aggregating the words or images into categories of information and presenting the diversity of ideas that were gathered during the data collection stage. Babbie and Mouton (2011:270) postulate that the main objective of this approach is to describe and comprehend rather than explain human behaviour. Neuman (2011:175) describes that qualitative research documents real events by recording what people say, observing specific behaviours, examining written documents and studying visual images.

Various scholars such as Neuman (2006) and Creswell (2014b) suggest that qualitative research is inductive in its approach. This means it generates theory from interpretation of the evidence, albeit against a theoretical background. Methods of qualitative research include observation, interviews, historical narrative, case study, documentary analysis and action research. Harwell (2011:128) denotes that this method focuses on discovering and understanding. Neuman (2013:165) and Leedy and Ormond (2005:135) associate qualitative approach with interpretivism for its capability to emphasise meanings (words) rather than frequencies and distributions (numbers) when collecting and analysing data. Such meanings are realised when collecting data where in-depth interviews, document and participant observation to understand and explain social and cultural phenomena (Creswell 2011).

Researchers that interpret qualitative data are aware that interpretive studies are idiographic, because they use a small number of participants. Leedy and Ormrod (2013:139) argue that the qualitative research approach in some disciplines (psychology and education) has been frowned upon for its subjective nature; however, it has recently regained wide acceptance as legitimate research. Bhattacherjee (2012:104) maintains that many positivist researchers view interpretive research as erroneous and biased, given the subjective nature of the qualitative data collection and interpretation process employed in such research. Furthermore, Patton (1990) points out the view that qualitative research focuses in depth on relatively small samples as well as single cases selected purposively. Patton (2005) contends that the intention of qualitative research is to achieve depth of understanding as opposed to the quantitative method, which is intended to achieve the breadth of understating.

According to Bhattacherjee (2012:44), qualitative data require qualitative data analysis techniques, such as coding. However, qualitative research is perceived weak and subjective. Creswell (2013) asserts that despite its perceived weakness of subjectivity, many studies that sought descriptive data have used qualitative methods, because they are able to generate ideas and concepts with in-depth focus on knowledge of the researcher's problem. The qualitative research approach is mainly used for brainstorming and testing new ideas. It gives participants the opportunity to verbally express their views pertaining to the current method used for records management and digital preservation. Ultimately, they are able to create a subjective balance between paper-based and digital record-keeping in the public sector. As already indicated, Bhattacherjee (2012) and Creswell (2014a) mention that the qualitative research method is

useful where a scholar seeks to comprehend the phenomenon by attaining illumination of the issues in order to produce meaning or theory based on the research findings. In this case, the study is not informed by predetermined variables, but the researcher starts to investigate a phenomenon with an open mind and depends on the opinions and response of participants to draw inferences and formulate a theory (Labaree 2013).

Hsiung (2012) and Mouton (2009) opine that the scholars use qualitative research methodology to enable an epistemological transformation that legitimizes multiple voices and varied realities in knowledge production. In this way, the scholars expect diverse responses that may elicit various interpretations of reality, because the data in qualitative research is not guided in any way, for example, closed-ended questions. . Data for this study are collected using face-to-face interviews and document analysis. Bearing in mind that the qualitative approach blends with the interpretivist method, data collection was sourced through interviews. Out of the views of the participants, the researcher was able to construct the meaning with the purpose of seeking to understand the world people live and work in (Creswell 2013). This is in line with Bryman (2007:19) and Neuman (2011:102) when they define qualitative research as an enquiry with an orientation towards social reality that assumes that people create and use fundamentally shape what reality is for them. The qualitative research paradigm can be summarised as follows:

- Understanding a phenomenon in a naturalistic or context-specific environment (Creswell 2013)
- Reliability and validity are conceptualised as "trustworthiness, rigour" and quality through triangulation (Neuman 2011).
- Increased involvement of researchers in the research process rather than disassociation.
- Analysis of results enjoys the compatibility of research methods such as interviews and observations with the reward of using both numbers and words (Leedy & Ormrod 2013).

The scholar employed qualitative research approach for the current study. Qualitative research approach provided an opportunity to interact with the participants in pursuit of their views in relation to the objectives of the current study.

3.4 Nature of research

The three common and useful types of research in social science are exploratory (explore a new topic), descriptive (describe a social phenomenon) and explanatory (explain why something occurs). Babbie (2010) and Neuman (2011:38) explain that exploratory research is often conducted in new areas of inquiry, where the goals of the research are: (1) to scope out the magnitude of a particular phenomenon, problem, or behaviour, (2) to generate some initial ideas about that phenomenon, or (3) to test the feasibility of undertaking a more extensive study regarding that phenomenon. Descriptive research focuses on description rather than examining relationships or association (Kumar 2005). It is directed at making careful observations and detailed documentation of a phenomenon of interest. According to Bhattacherjee (2012:6) and Neuman (2013:38), these observations are based on the scientific method, for example, it must be replicable as well as precise, and are more reliable than casual observations by untrained people. The authors further indicate that explanatory research seeks explanations of observed phenomena, problems or behaviours.

While descriptive research is used to examine what, where and when of a phenomenon, explanatory research solicits responses to why and how of questions. It endeavours to connect the dots in research by identifying casual factors and outcomes of the target phenomenon. Furthermore, Ngoepe (2012:90) suggests that although a given study can have more than one of these types, examining them separately is useful as each has different implications for other aspects of research design. This study applied exploratory methods. Taking a closer look into the purpose of the study, this selection was motivated by the fact of exploring the ways that are used for current data storage and describing how the proposed cloud storage could improve the current records management in the public sector. It explored how migrating from the current paper-based records keeping to digital preservation in the cloud could enhance e-government services.

3.5 Research methods

Babbie and Mouton (2011:270) advise that research methods should be selected to best fit the problem statement of the study and not the other way round. This section discussed which research method the researcher employed for collecting data in order to address the research questions of interest of this study. Mouton (2009) notes that the research methods are linked to

either the positivist or the interpretive paradigm; for example, the popular research methods linked to the positivist paradigm are laboratory experiments, field experiments, field surveys, secondary data analysis and case research for their essence of supporting theory testing. In the contrary, research methods in no particular order linking to interpretive design are case study, ethnography, phenomenology and grounded theory in support of theory building. Considering that this is a qualitative study, explanation of research methods linking to positivism were intentionally omitted for their quantitative nature in favour of interpretivism.

3.5.1 Case study

Yin (2017) defines case study as an empirical enquiry about a contemporary phenomenon, set within its real-world context especially when the boundaries between phenomenon and context are not clearly evident. It comprises the full set of procedures needed to do the case study research such as data collection, data analysis, as well as presenting reporting he results. The author also postulate that as a by-product and a final feature in appreciating case study research, the relevant case study data are likely to come from multiple and not singular source of evidence. Bhattacherjee (2012) argues that researchers prefer to choose research methods or design that they are most content with and feel more competent to manage. However, that should not be the case, because research method is reliant on the nature of the research phenomenon that is studied. In the event where the research problem is unclear and the researcher wants to scope out the nature and extent of a certain research problem, a focus group or case study is an ideal strategy for exploratory research. A focus group chiefly targets an individual unit of analysis while a case study focuses on organisational unit of analysis. In this study, case study has been selected, because organisational unit of analysis has been targeted as a source of relevant data in relation to the objectives of the study. The organisational unit of analysis is formed by the CIOs and archive/records practitioners from the national government departments of South Africa. These organisational units of analysis have in-depth knowledge of record keeping since it affects them directly.

Bhattacherjee (2012) defines case study or idiographic research as a method of intensively studying a phenomenon over time within its natural setting in or a few sites. On the other hand, Leedy and Ormrod (2010) explain that in a case study, a particular individual, programme or event is studied in depth for a defined period of time. It is a formal research technique that involves a scientific method to derive explanations of organisational phenomena (Babbie &

Mouton 2011). This is suitable for learning more about a little-known or a poorly understood situation. Normally, a case study researcher embarks on data analysis process during data collection; preliminary conclusions are likely to influence the kinds of data the researcher seeks out and collects in later study (Leedy & Ormrod 2013). Furthermore, case study is interpretive in nature. This means it is an inductive technique where evidence collected from one or more case sites is systematically analysed and synthesised to allow concepts and patterns to emerge for the purpose of building new theories or expanding existing ones. Various authors such as Leedy and Ormrod (2013), Creswell (2013) and Neuman (2013 mention the following prominent advantages of case study:

- theory building or theory testing
- research questions can be modified during the research process if the original questions are found to be less relevant or salient
- derive richer, more contextualised, and more authentic interpretation of the phenomenon of interest than most other research methods by virtue of its ability to capture a rich array of contextual data
- The phenomenon of interest can be studied from the perspectives of multiple participants and using multiple levels of analysis

Despite its strengths, Bhattacherjee (2012) contends that case study is a difficult research method that requires advanced research skills on the part of the researcher and is often prone to error. In the same breath, Benbasat, Goldstein and Mead (1987) contends that case study has its inherent weaknesses just like any other research method. This is influenced by the fact that it does not involve experimental control, which leads inferences of internal validity to remain weak. These authors list some of the following problems that are experienced in case study:

- Starting without specific research questions and end up without specific inferences.
- Selection is based on convenience than on the fit with research questions.
- Researchers do not validate or triangulate data collected using multiple means, which leads to biased interpretation based on responses from participants.
- Studies provide little details on how data was collected.

However, its problems can be addressed using natural controls. Based on the experiences possessed by the participants that were purposively selected for the interviews, case study was useful in this study.

3.6 Data collection tools

Data collection is a crucial component to conducting research. Saunders et al (2009) postulate that data collection is considered as a social interaction that involves the researcher and the participants and it is analysed by using any or a combination of the research purpose – descriptive, exploratory, predictive, or analytical. Bernard (2002) opines that it contributes to a better comprehension of theoretical framework, because it is steered by the existing theories. According to Creswell (2013), two sources of data are distinguished as primary data (arise directly from original sources like interviews, observation or questionnaires) and secondary data (consist of materials that come from someone other than the original source, for example, a published book). Stacks and Hocking (1992) as cited by Ngoepe (2012), explain that a third source of data is tertiary data (consist of interpretation of or comments on secondary sources, for example, book review).

According to Ngulube, Mathipa and Gumbo (2015), the commonly used instruments to collect data are questionnaires, interviews, observation and document analysis. These instruments can be applied to both quantitative and qualitative paradigms, depending on the selected research approach. However, Locke, Silverman and Spirduso (2010) and Creswell (2009) indicate that interview, observation and document reviews are the most common sources of data collection in qualitative research. While qualitative research frequently relies on interviews, quantitative research relies on numbers. Given the fact that this is a qualitative research, data were collected through semi-structured interviews and document analysis where policies and legislations on records management were reviewed. See interview questions on Appendix A.

The next section discusses each instrument of data collection that was used in this study. An interview guide that introduces the topic of discussion and a consent form was provided to the participants before the beginning of each interview. While all the participants were asked the same basic questions, which were prepared in advance, the exact wording and sequence of questions were determined during the course of the interviews. The participants were assured that any data used for publication would remain anonymous.

3.6.1 Interviews

Rubin and Rubin (2012) assert that interviews provide researchers with rich and detailed qualitative data for understanding participants' experiences, how they describe those experiences, and the meaning they make of those experiences. Due to the qualitative nature of this study, interviews were an appropriate method because of the need to collect in-depth information on the target population's opinions, thoughts, experiences, and feelings (Gubrium & Holstein 2001). Bhattacherjee (2012) suggests that interviews are a more personalised method of data collection than questionnaires, and are conducted by trained interviewers using the same research protocol as questionnaire surveys. Creswell (2013) points out that qualitative approach is inductive with specific instances used to arrive at overall generalisation. Interviews, as closely related to qualitative research, help researchers to collect and analyse soft data in the form of text, pictures, audio and video in order to establish the findings. This is informed by the fact that an interview is a social relationship designed to exchange information between the participant and the researcher. Monette, Sullivan and Dejong (2011:178) concur that the quantity and quality of information exchanged would depend on how astute and creative the interviewer is at comprehending and guiding the relationship. Bhattacherjee (2012:109) indicates that in the data collection phase, participants embedded in a social phenomenon are interviewed to capture their subjective experiences and perspectives regarding the phenomenon under investigation.

Babbie and Mouton (2011) and Neuman (2007) suggest that the most typical form of interview is personal or face-to-face interview, where the interviewer works directly with the participant to ask questions and record their responses. Face-to-face interviews are suitable when the target population can communicate through face-to-face conversations better than they can communicate through writing or phone conversations (Gubrium & Holstein 2001). Interviews for social research are either structured or semi-structured and appropriate when the study is aimed at attaining individual views, beliefs and feelings about a subject.

Bradford and Cullen (2012) assert that semi-structured interviews, as preferred for this study, are one of the most dominant and widely used methods of data collection within social sciences. Leedy and Ormrod (2013) further explain that semi-structured interviews are applicable where a researcher follows the standard questions with one or more individually tailored questions to get clarification or probe a person's reasoning. Choak (2012) mentions that they enable

researchers to explore subjective viewpoints and to gather in-depth accounts of people's experiences. The author further elaborated that a typical interview schedule is used to enable researchers to address a defined topic whilst allowing the participants to answer in their own terms and to discuss issues and topics pertinent to them. Evans (2018) points out that the popularity of semi-structured interviews within the social sciences partly reflects their independence from a single theoretical framework or epistemological position. Braun and Clarke as cited by Evans (2018) indicate that these interviews are useful to consider experience, meanings, and the reality of participants' experiences as they can be used to explore how these experiences, realities and meanings might be informed by discourses, assumptions or ideas that exist in wider society.

Unstructured interviews employ unstructured questionnaires containing a number of open-ended questions whose wording and order can be changed at will (Sarantakos 2013:278). Such interviews are extremely flexible and do not limit the field of enquiry. On the other hand, the author postulates that semi-structured interviews allow the researcher to have a list of questions addressing the topic to be covered which is used with all interviewees, but mostly as a guideline, because the researcher may choose to ignore some questions or even add other questions during the interview session if necessary. However, Bhattacherjee (2012:78) contends that interviews are time-consuming and resource intensive. Singleton and Straits (2010) indicate that the interview technique, as a method of collecting data, has various advantages, such as more accurate responses, because of contextual naturalness; a greater likelihood of self-generated answers; a symmetrical distribution of interactive power and greater effectiveness with complex issues. The interviews for this study were arranged according to the objectives and where necessary, follow-up questions were asked to obtain the in-depth information. To provide quality to the study, questions were asked randomly depending on the responses provided by the participants. The benefits and limitations of interviews are summarily discussed below.

3.6.2 Benefits of interviews

According to Sarantakos (2013), interviews are well-suited for exploring concealed details behind intricate, interrelated, or multifaceted social processes, like inter-firm relationships or inter-office politics, where quantitative evidence may be biased, erroneous, or otherwise challenging to attain. In the same breath, the author suggests that interviews allow the

participants to provide information in some depth using their own words, which assists the scholar to gain a real sense and comprehending of a particular situation. However, that is reliant on their comfort during the interviewing process. Leedy and Ormrod (2013) observe the interviews have the potential for theory building in areas with insufficient prior theory. These scholars further suggest that interviews are appropriate for studying context-specific, idiosyncratic events or processes and help to reveal interesting and relevant research questions and issues for follow-up research. Interestingly, unstructured interviews also have the potential to produce accurate information, because the interviewer has the opportunity to probe for deeper understanding by asking follow-up questions for clarity during the interview.

3.6.3 Limitations of interviews

Bhattacherjee (2012) shows concern that interviews are more time and resource intensive. The author points out that too little data can lead to false or premature assumptions, while the researcher may not effectively process too much data. The author also suggests that interviews require a well-trained interviewer who is capable of seeing and interpreting intricate social phenomena from the perspectives of the embedded participants and reconciling the varied perspectives of these participants, without injecting their personal biases or preconceptions into their inferences. All participants or data sources may not be equally credible, unbiased, or knowledgeable about the phenomenon of interest, or may have undisclosed political agendas, which may lead to misleading or false impressions. Given the heavily contextualised nature of conclusions drawn from interpretive study, such conclusions do not lend themselves well to replicability or generalisability. At some point, interviews are incapable to answer the research questions of interest or predict future behaviours. Mouton (2009) reminds scholars that it takes longer to conduct an interview and analysing the data obtained is time consuming. It is also costly to gather data in this way, particularly in cases where extra people may be needed to provide assistance.

3.6.2 Content analysis

Content analysis is a detailed and systematic examination of the contents of a particular body of material for the purpose of identifying patterns, themes or biases (Leedy & Ormrod 2013). This is performed on forms of human communications, including books, newspapers, legal documents like policies that may be used to cast further insight into the phenomenon of interest

or to corroborate other forms of evidence (Bhattacherjee 2012; Bryman 2012:543). Maluleka (2017) points out that the official documents commonly used in social science research include government documents such as policy documents, and any other official report that may be of value to the research. This study consulted government Acts and government policy documents, particularly those discussing and providing information of records management. These were available on the websites and government departments were physically visited to request for policies in line with this study.

Sarantakos (2013) lists some of the following advantages of document analysis: retrospectivity – a documentary method that consents the scholar to research historical events; quick and easy to access – a documentary research that is free of the restrictions, difficulties and problems faced during data collection from participants. The author also mentions the following limitations: lack of representativeness – documents are not necessarily representative of their kind and do not allow generalisation; personal bias – documents may be biased since they represent the views of their authors; incomplete data – some documents are not complete or up to date. It should be noted that this study required a review of policies that were used in the records management environment of each selected department in order to identify the efficiency with regard to the government's vision of e-government.

3.7 Research procedures

According to Creswell (2014a) and Cooper and Schindler (2008), research procedures typically include the population and how it was obtained, sampling procedures, instrumentation used, procedures employed in gathering and processing data, and statistical treatment of data. Banerjee and Chaundry (2012) and Cooper and Hedges (1994) postulate that regardless of quantitative or qualitative research, a population refers to the total of subjects that bear a common characteristic that would be of interest to the researcher out of which the researcher extracts a small fraction, the sample that becomes the actual participants to the study who provide the data to the study. People reading research products are entitled to know how the procedures were followed to conduct the study. As already indicated, research design is a blueprint that intends specifying which research questions must be answered, how and when the data will be gathered, and how the data will be analysed, research procedures reflect how the study arrived at the findings (Bhattacherjee 2012:21).

3.7.1 Population of the study

Bhattacherjee (2012) defines population as all people or items with the characteristics that one wishes to study. Neuman (2011) also defines population as an abstract idea of a large group of many cases from which a researcher draws a sample and to which results from a sample are generalised. Sampling process comprises several stages where the first stage is to define the target population or unit of analysis. Depending on the research being conducted, the target population may be a person, group, organisation, country, object, or any other entity that you wish to draw scientific inferences about. It is not a coincidence that Bhattacherjee (2012:22) and Babbie and Mouton (2011) advise researchers to carefully choose the target population from which they wish to collect data, and a sampling strategy to select a sample from that population. The target population of this study constitutes CIOs and archive/records practitioners purposively selected from the national government departments of South Africa. These people have expertise in their respective areas of competency, for example, IT and records services within their organisations. The CIOs have capability to influence the virtual storage of the organisation's records. The records practitioners are responsible for the footprints of the organisation by ensuring that records are stored and remain authentic. In the evolution of technology, they rely on CIOs to intervene when storage formats change.

Singleton and Straits (2010:155) further advise that in order to define the target population, the researcher must specify the criteria for determining which cases are included in the population and which are excluded. Each participant was assigned a number, for example Participant A, to be identified by. The interviews were conducted in their offices in English. Although English is not the first language of some participants, all of them were fluent. The interviews lasted between 30 and 45 minutes. All the interview sessions were audio-recorded (see the list of questions that were used in Appendix A).

As already indicated in the data collection section, Bernard (2002) suggested that data gathering is crucial in research, as data are meant to contribute to a better understanding of a theoretical framework. Etikan, Musa and Alkassim (2016) further elaborate that it then becomes imperious that selecting the manner of obtaining data and from whom the data is acquired be done with sound judgement, especially since no amount of analysis can make up for improperly collected data. Simply put, the researcher decided what needed to be known and

set out to find people and organisations that were willing to provide the information by virtue of knowledge or experience. Patton (2002) indicates that it is typically used in qualitative research to identify and select the information-rich cases for the most proper utilisation of available resources. Creswell and Plano-Clark (2011) mention that this involves identification and selection of individuals or groups of individuals that are proficient and well informed with a phenomenon of interest. Supporting the above explanation, purposive selection was relevant for this study given the qualities possessed by the participants. Having defined target population, the next section discusses the sampling procedures followed in this study.

3.7.2 Sampling

The second step in the sampling process is to select a sampling frame using a well-defined sampling technique, which can be grouped into probability (random) sampling and non-probability sampling (Bhattacherjee 2012:66). Probability sampling is a technique in which every unit in the population has a chance (non-zero probability) of being selected in the sample, and this chance can be accurately determined. Advantageously, this sampling technique removes the possibility that the researcher's biases will affect the selection of cases. Secondly, it is by virtue of random selection that the law of mathematical probability may be applied to estimate the accuracy of the sample. Probability sampling provides a researcher with an advantage to know to which population the sample may be generalized, as well as the limits of generalisability. Sample statistics produced, such as sample mean or standard deviation, are unbiased estimates of population parameters, as long as the sampled units are weighted according to their probability of selection. All probability samplings have two attributes in common: 1(1) every unit in the population has a known non-zero probability of being sampled, and (2) the sampling procedure involves random selection at some point.

Non-probability sampling is a sampling technique in which some units of the population have a zero chance of selection or where the probability of selection cannot be accurately determined. As opposed to probability sampling, non-probability population is undefined and the laws of probability do not apply. Typically, units of analysis are selected based on certain non-random criteria, such as quota or convenience. Because selection is non-random, non-probability sampling does not allow the estimation of sampling errors, and may be subjected to sampling bias. The information from a sample cannot be generalised back to the population.

Neuman (2006) notes that researchers normally do sampling to save time, costs, and to produce accurate results. Sampling is an accessible section of the target population (usually a list with contact information) from where a sample can be drawn. According to Mouton (2009), sampling is the statistical process of selecting a subset (called a "sample") of a population of interest for purposes of making observations and statistical inferences about that population. According to Singleton and Straits as cited by Ngoepe (2012:100), it is advisable for researchers to obtain a clear picture of the population before selecting the sample, starting from the top (population) and working down (to the sample), as against working from the bottom up to the top. Neuman (2007:219) defines sampling as a process of having a small collection of units from a large population to allow the researcher to study the smaller group and produce accurate generalisation about the larger group. It is important to note that generalisation is a preoccupation of quantitative research and in qualitative studies like the current study, the researchers are not obliged to ensure things like sample representativeness, because the results are not going to be generalised.

The purposive selection of these institutions is justified as follows:

- NARSSA fosters a national identity and the protection of rights by preserving a national archival heritage for use by the government and people of South Africa. This institution, through the National Archivist, provides guidelines of records management to the government departments.
- DAC develops and preserves the South African culture to endure social cohesion and nation-building. It is again the tasked with the preservation of national heritage.
- SITA is a state-owned entity that was established to streamline existing technologies and to implement new systems in all government departments. It is a company that provides IT information systems (IS) and related services to the government (Kroukamp 2005).
- The DBE translates government's education and training policies and the provisions of the constitution into a national education policy and legislative framework. In it, cloud storage is crucial for the students for easy interaction with the department.
- The DHET provides national strategic leadership in support of post-school education and training system for improved quality of South Africa. Therefore, its records are crucial to the academic institutions and the students.

Various researchers such as Neuman (2011), Sarantakos (2013) and Gerring (2012:74) espouse

that the following sampling techniques: accidental sampling, purposive sampling, quota sampling, snowball sampling, sequential sampling, theoretical sampling, and adaptive sampling are some of the main non-probability sampling techniques that can be used in qualitative studies. Accidental sampling is a procedure that employs no strategies or techniques to choose participants. The researchers use all cases that they accidentally encounter during data collection. It is called accidental sampling, because the participants are selected by accident (unplanned) and happen to be there when the researcher is doing the investigation. Quota sampling is a technique where the investigator sets a proportion of participants to be chosen from specific population groups. The researcher sets a number of cases to be selected for each category within the population to represent different dimensions of the population.

In snowball sampling, the researcher uses any other sampling technique to select the first group of participants and then asks them to recommend other people who meet the criteria of research and who might be willing to participate. This referral process may be continued until data saturation is reached. The sequential sampling technique is similar to purposive sampling. The known significance difference is that sequential sampling gathers cases until the amount of new information ends or when saturation is reached. Theoretical sampling is the process of collecting data in order to generate a theory. The knowledge gained from the first participant informs the researcher who will be the next suitable participant for interview. With these interviews, the investigator gains knowledge about the research topic. Adaptive sampling is a technique used for hidden populations where different sampling techniques can be used in the beginning.

Having started by discussing literature of sampling, this study employs purposive sampling technique wherein the CIOs and records practitioners are purposively selected from government departments. This selection is justified by the specialised skills these people possess in the field of technology and records management. For example, the records practitioners are involved on the day-to-day operations of records management services. The CIOs are selected with the premise that they are responsible for the IT strategies for the organisations. They are the decision-makers on the directions records should take in response to the widespread evolution of digital transformation. They understand better how the organisations can save costs and provide ubiquitous access of records by using cloud storage. The combination of CIO with records practitioners is informed by cloud platform that CIOs pave way for while records practitioners concentrate in records management as a whole. The

CIOs are capable to select the best cloud models that records practitioners can use to the benefit the organisation. In some organisations, that led to the selection of three participants, for example, a CIO and two records practitioners. The total number selected was ten participants from IT and records services sections of the national government departments. Some of the challenges experienced during selection were caused by the change of plans by the participants without notice. Some would avail themselves but change minds indicating that they have other urgent matters that required their attention. Others would instead refer the researcher to someone with similar competitive expertise within their directorates for their replacement.

3.8 Trustworthiness and authenticity of data

According to Bhattacherjee (2012) and Bryman (2012), the quality of qualitative research studies is assessed through its trustworthiness and authenticity. Bryman (2012) also espouses that as opposed to quantitative research study, which concentrates on reliability and validity to establish and assess its quality through measurements, qualitative research is reliant on trustworthiness and authenticity. Ngoepe (2012:111) indicates that the correct usage of data collection instruments in qualitative study guarantees authenticity and trustworthiness of data. Other scholars such as Ndenje-Sichalwe (2010) and Yin (2009) opine that the quality of a research study depends to a large extent on the accuracy of the data collection procedures. The next two paragraphs provide the distinctions between trustworthiness and authenticity of data.

3.8.1 Trustworthiness

Bryman (2012) postulates that trustworthiness is made up of four criteria and each one of them has an equivalent in qualitative research:

- Credibility – parallels internal validity and is about guaranteeing that the research is carried out in the correct way and the results are confirmed by the participants to show that the researcher comprehended the social world of that population. This is applicable when the researcher revisited the participants to verify with them if their responses were not misunderstood or misinterpreted.
- Transferability – parallels external validity and is about producing detailed accounts of the social world rather than focusing on coverage.
- Dependability – parallels reliability and is about keeping record of all phases of the

research to establish how well proper procedures are being and have been followed.

- Conformability – parallels objectivity and is about ensuring that the objective of the scholar has avoided personal feelings, values or perceptions to sway the conduct of the research and the findings thereof. The responses are recorded as they are, and to check that the researcher listened to the tapes confirming what had been said and what was presented in the document. In order to boost recording, field notes are taken.

Given the nature of this study, data were collected from CIOs and archives/records practitioners from various government departments. These were considered to have first-hand information in terms of ICT strategy, legislation as well as day-to-day operations of records management. The researcher ensured that credibility was adhered to through uninterrupted audio-recording with an audio-recorder. The researcher then triangulated the recording with the records management documents that were analysed during the process.

3.8.2 Authenticity

Authenticity is closely linked to credibility and is concerned with the correct interpretations of experiences of the selected participants for this study (Bhattacherjee 2012). Bryman (2012) points out that the following characteristics are significant to authenticity in qualitative research:

- Fairness – the research should fairly represent different viewpoints of the participants.
- Ontological authenticity – the research should help the population to understand their social world better.
- Educative authenticity – the research should teach other members to appreciate the perspectives of other members in their social world.
- Catalytic authenticity – the research should have an influence on members to the possibility of changing their circumstances.
- Tactical authenticity – the research should empower members to take action in their social world.

Following the collection of data, the researcher listened and reworked them by transcribing audio to the paper. After transcription, the researcher revisited the participants for further clarity. To ensure accuracy, the audio-records were listened to again and the transcripts

inspected for errors. To ensure authenticity, the researcher revisited some participants in order to share with them what was captured and allowed them to make further comments. This ensured that any misunderstanding during interpretation was rectified. In a qualitative study, authenticity is linked to credibility which was discussed under trustworthiness (3.8.1) and involves correct interpretations of correct expertise of the participants of this study.

3.9 Data analysis and presentation

Following data collection through semi-structured interviews and document analysis, the data are analysed and interpreted for the purpose of drawing inferences regarding the research questions of interest (Bhattacherjee 2012). The data collected were in the form of text from document analysis, interview transcripts and audio-recordings obtained from interviews, which were thematically analysed. The data obtained from these sources were integrated and grouped in an effort to answer research questions in section 1.4. Thematic analysis is a common approach to qualitative data analysis (Bryman 2012). Braun and Clarke (2006) mention that thematic analysis as an independent qualitative descriptive approach is mainly described as a method for identifying, analysing and reporting patterns (themes) within data. Furthermore, Evans (2018) explains that thematic analysis must be employed if a researcher is interested in examining the ways that people make meaning out of their experiences, as well as how they construct their social worlds through meaning-making, but also require to retain focus on the ways in which these experiences will be informed by their material experiences and contexts.

3.9.1 Thematic analysis

According to Braun and Clarke (2006) and Clarke and Braun (2013), thematic analysis is a process of identifying patterns or themes within qualitative data. It can be called a method instead of a methodology. Evans (2018) points out that this begins at the stage of data collection and continues throughout the process of transcribing, reading and re-reading, analysing and interpreting the data. The author emphasised that unlike many qualitative methodologies, it is not tied to a particular epistemological or theoretical perspective. Despite many different ways to approach thematic analysis, this study followed the six-step framework of Braun & Clarke (2006). This six-step framework is arguably the most influential approach, in the social sciences at least, because it offers such a clear and usable framework for doing thematic analysis (Evans 2018). Clarke and Braun (2013) indicate that the goal of a thematic analysis is

to identify themes, meaning patterns in the data that are important or interesting, and use these themes to address the research or say something about an issue. This is much more than simply summarising the data; a good thematic analysis interprets and makes sense of it.

Manually, the six steps of thematic analysis were applied as follows:

1. Familiarisation with data: the researcher used this step to listen to the recordings of the interviews. Considering that interviews were held once in a while due to the availability of participant, the researcher would listen to the available recording before meeting the next one. This gave more time to listen repeatedly. Field notes were read in conjunction with the hearing of the recordings in order to remember how they relate to each other. That was followed by transcribing data and listening over again to ensure that words are not misheard.
2. Generating of initial codes: In this step, interesting words from the recordings were underlined and highlighted as a way of creating codes in line with sets of data. This was done manually by writing notes, highlighting and underlining for analysis.
3. Searching for themes: In this stage, codes were sorted into potential themes. This stage reflected related themes that would be grouped together. Candidate themes and sub-themes have been collected into their relations.
4. Reviewing themes: Candidate themes were refined in order to create headings. The researcher generated a thematic map of analysis according to their relevance.
5. Defining and naming themes: In this stage, themes were defined and refined in order to analyse data within them. This identified the essence of what each theme represented. This gave a researcher an opportunity to define and name each theme that was generated.
6. Producing the report: this step helped the researcher to provide or select coherent and non-repetitive data within and across themes. A report for analysis was produced on each themes.

Clarke and Braun (2013) contend that a common pitfall for researchers is to use the main interview questions as the themes which typically reflect the fact that data have been summarised and organised, rather than analysed. The two main approaches to analysis of qualitative data are deductive (top down) and inductive (bottom up) approaches. According to Braun and Clarke (2006), these approaches are used to identify themes or patterns within data. In the deductive approach, the scholar has a predetermined framework to help in the analysis

of data. Deductive approach allows the scholar to impose theory or framework in the analysis. In the contrary, inductive approach does not have a predetermined structure and the researcher uses the data collected to derive the structure of analysis.

The primary purpose of the inductive approach is to allow research findings to emerge from the frequent, dominant or significant themes inherent in raw data, without the restraints imposed by structured methodologies. Thematic analysis is an inductive approach and is more predominant and common in qualitative studies (Braun & Clarke 2006). The benefit of thematic analysis is its flexibility and this makes it a foundational method for qualitative analysis. Anderson (2015) concurs that thematic analysis is most appropriate when data are collected through interviews, like in the present study. Data presentation was done according to the research themes derived from the research objectives and research questions. Fundamental to the nature of this study is the capture of the participants' voices in presenting data where verbatim and substantive quotations have been extracted and presented to reveal participants' opinions. This is essential not only in enhancing reliability of the data, but also in demonstrating the in-depth understanding of the phenomenon under investigation, which is central to the study (Ambira 2016).

3.10 Ethical considerations

According to Johnson and Christensen (2008:109) Klein and Myers (1999), ethical research embodies informed consent, privacy and confidentiality as well as protection from harm. When conducting a social science study, the researchers are expected to adhere to a number of strict research ethics. In both qualitative and quantitative research, researchers face ethical issues that surface during data collection in the field and in analysis and dissemination of research reports (Creswell 2006). Ethical considerations are important in a study because science has often been manipulated in unethical ways by people and organisations that seek to advance their private agenda and engage in activities that are contrary to the norms of scientific conduct. Bhattacherjee (2012) defines ethics as the moral distinction between right and wrong, and what is unethical may not necessarily be illegal. Researchers have an obligation to maintain confidentiality of their participants. Singleton and Straits as cited by Ngoepe (2012) opine that there are three broad areas of ethical concerns in scientific research: the ethics of data collection and analysis, the ethics of treatment of participants as well as the ethics of responsibility to society. A crucial ethical rule governing research on humans is that participants must give their

informed consent before taking part in the study (Neuman 2011). Ngoepe (2012) emphasises that researchers have an obligation to maintain the confidentiality of their participants. Like any other institution, UNISA has created its own research ethics policy (2007) that adds greater protection for subjects. The policy states that the rights and interests of human participants should be protected in research.

Creswell (2013) propounds that during the process of planning and designing a qualitative study, scholars need to consider what ethical issues might surface and plan how to address them. Stevens (2013) asserts that ethical considerations are noteworthy to qualitative research, because the unstructured nature of interactions between a scholar and the participants can be indiscreetly personal and highly interactive. It is for this reason that Creswell (2002) recommends that ethical considerations should be assessed at various stages of a study, at the beginning of research, during data collection, during data analysis and in publishing the findings. At the beginning of data collection, Leedy and Ormrod (2013) advise that the scholar should make known the purpose of the study. Creswell (2013) postulates that disclosing the purpose of a study is important in securing voluntary participation by intended participants and also to avoid placing participants under undue stress. In the current study, the scholar secured participation of the target population by first making request through the relevant sections, for example, Research Section of the purposively selected government departments. In that request, the purpose of the study was declared. That way simplified appointments for interviews with the participants, for example, CIOs and records practitioners. Appointments were secured through electronic mail, personal visits and telephone conversations. The similar information that was declared to the sections that granted permission to conduct research for the current study was declared again to the participants. Plano-Clark (2010) indicates that during the actual data collection, participants should not be deceived. Informed consent should be obtained from participants and there should be as minimal disruptions to participants' lives as possible (see Appendix B for participants' consent to interviews). It should be noted that the purpose of securing appointments with the participants even though their Research Section has already granted permission was in cognisant of the fact that the participants are full-time employees and they might have other work commitments. This ensured that the interviews did not interrupt the schedules of the participants. At the start of every interview session, the researcher explained the purpose of the study and the nature of information required.

Creswell (1998) cautions against disclosing information that would harm participants and/or

constitute plagiarism when analysing and reporting research findings. Participants must be afforded respect. This study maintained the identities of all participants as confidential and endeavoured not to disclose their privacy. Creswell (2002; 2013) highly recognises the publication of the research findings. It is crucial to share a research study with stakeholders, including the participants, potential industry beneficiaries and professional colleagues. In the present study, the scholar has consented to unlimited provision of the research report to any interested parties through the university channels, both in hard copy and electronic formats.

The UNISA Policy on Research Ethic (2007) stipulates that all researches must be conducted ethically at all times and the rights and interests of all participants must be protected at all times. Considering that the current study conducted face-to-face interviews and document analysis, Bhattacherjee (2012:79) advised that a scholar should carry a letter from the supervisor for participants to call and verify the interviewer's authenticity. Guaranteeing anonymity and confidentiality protected the right to privacy of the participants. Ethical clearance was obtained from the Department of Information Science's ethics review committee (see the ethical clearance document in Appendix C). In the current study, each participant was informed as to who was conducting the research and that participation was voluntary. Bhattacherjee (2012) recommends that each interviewee must be informed who is conducting the research, why they were invited to participate, that participation is voluntary and they are free to withdraw at any time, and that anonymity and confidentiality would be maintained at all times. Considering that document analysis formed part of this study, all legislative documents consulted were acknowledged to avoid plagiarism. Bailey (2007:24) points out that it is the responsibility of a researcher to assure personal confidentiality of all participants and those participating in a study. As supported by Neville (2010) this thesis was also subjected to Turnitin in order to minimise similarity on indexing and referencing of consulted sources.

3.11 Research methodology evaluation

Scholars are expected to evaluate research methodologies applied with a view of outlining the strength and weaknesses in the study. This study applied qualitative research where interviews and document analysis were employed for data collection. Creswell and Zhang (2009) hold that the main strength of qualitative approach reflects in the depth to which explorations are conducted and descriptions are written. According to Leedy and Ormrod (2010), research methods are not perfect and their imperfections continuously cast doubts on the findings. The

study relied on interviews from well-informed participants in record-keeping space and legislative documents used in their institutions. However, some participants arranged the meeting, but changed due to other commitments before we could reach the fourth question. They never availed themselves again on the date they rescheduled the meeting for interview. Instead, they assigned their assistants who work directly with the records. Furthermore, the researcher would have liked to add more participants from other three departments, for example, DHA, DST and DTPS, but the internal administrative process to conduct interviews took too long to be approved despite follow-ups. The DHA through the Deputy Director-General of Human Resources Management and Development granted permission to conduct interviews, but the interviewees never accepted. The DST kept on saying that the follow up on granting approval is underway, but that never happened despite many follow ups that were made through emails and telephone calls by this researcher. The DTPS too acknowledged the acknowledge receipt of the communiqué, which was referred to the Administration branch for attention however, that also proved futile despite telephone calls and emails that were made. Some interviewees were unintentionally dishonest when answering some questions. This was noticed during the progress of the interview or when interviewing another participant from another section. The unreliable and dishonest information was not used for this study. For instance, they would claim that there are no policies for record-keeping irrespective of digital and paper-based practice while others would provide the old documents. Content analysis proved futile some organisations, particularly in policies, as some CIOs were reluctant to make policies available. They were suspicious that the researcher wanted to implement it in another working environment. However, the researcher had to explain again and provided the original ethics clearance that we had to go through it together to prove that the request form part academic and it is important to ascertain the information. That yielded a policy on records management from registry and ICT security policy from the CIOs. The records management policies provided were derived from NARSA Act of 1996 and nowhere did they mention cloud with the exception of digital records stored on the servers and external hard-drives.

3.12 Summary

The chapter explained the research methodology followed to conduct the current study in order to enable future researchers to avoid challenges faced by the current study. It addressed study population. Sampling, data collection, data analysis, data presentation and ethical

considerations. It went further to provide an overall evaluation of the methodology and the researcher's view of the methodology's effectiveness in achieving the objectives of this study.

CHAPTER FOUR

DATA ANALYSIS AND PRESENTATION OF FINDINGS

4.1 Introduction

The previous chapter discussed the research methodology used to conduct the current study. It focused on the ways the researcher followed to address the research objectives. This chapter analyses data and presents the findings collected from the target population through semi-structured interviews and document reviews. De Vos, Strydom, Fouche and Delport (2011) opine that the presentation and analysis of findings are crucial because scholars are permitted to reduce collected data to an intelligible and interpretable form so that the relations of problems are easily studied and tested to the point where conclusions are drawn. The presentation of results as guided by the objectives of this study were arranged according to the following themes:

- Analyse policies and legislative frameworks used for records storage in the cloud in order to support e-government services.
- Determine if the public sector entrusts records in the cloud storage.
- Analyse the public sector's view on digital preservation of records.
- Determine the processes followed to dispose records in the cloud.
- Propose a framework that guides storage of records on the cloud in South Africa.

4.2 Presentation and analysis of data

Leedy and Ormrod (2013) and Saldana (2013) recommend that during the presentation of data, researchers are expected to think as spectators rather than as presenters in order to mitigate bias. Neuman (1991) suggests that for qualitative research, scholars should concentrate less on the sample's representativeness and rather on how the sample or small collection of cases, units or activities illuminate social life. This is informed by the fact qualitative researches are popular in producing deep data (inductive) and not statistical data that is synonymous with quantitative studies. Given the qualitative nature of this study, data were reduced without losing the meaning. Creswell (2009) further recommends that at least 5 to 25 participants should be interviewed. On the other hand, Creswell (1998) points out that interviews are reliant on when saturation is reached. The current study reached saturation after collecting data from ten crucial

participants in IT and records management sections. However, it should be noted that despite having ten participants, any participant who did not have a response or repeated an answer was omitted in the presentation of data. Furthermore, the researcher integrated similar responses provided by the participants.

In line with ethical considerations, the researcher started by explaining the purpose of the study to all participants. Leedy and Ormrod (2013) state that the object of enquiry in social science research is the human being and as such, extreme care should be taken to avoid causing any harm. The researcher reminded the participants that their participation was voluntary and that they had a right to discontinue the engagement at any point felt uncomfortable during the interview process. The participants were guaranteed anonymity and confidentiality of their participation. In addition to their privacy, participants had their names coded as "participant" in order to enhance their anonymity. All the interviews were conducted in English at the participants' workplace at the times and days they determined appropriate. As already indicated in section 5.7.1, unit of analysis of this study was made up of CIOs and records practitioners. The total interviews held were ten where four CIOs and nine records practitioners were interviewed from the purposively selected government departments as indicated in section 3.7.2. It should be noted that the number could have been more, but some participants from other departments decided to cancel at the last minute. The interviews took approximately 45 minutes. All the interviewees were given codes, for example Participant A, B, C, which replaced their names in order to ensure anonymity. Table 4.1 describes roles of the anonymised participants. Following the gathered data through interviews and content analysis, data were thematically analysed and that took a full month. Only one participant declined to be recorded, but offered to speak slowly in order to give the researcher the opportunity to take notes.

Despite guaranteeing confidentiality of all participants, he indicated his measure of dissatisfaction with recordings. He added that it is not easy for him to trust investigators with his recorded voice. He explained that the researcher presented the data in a way that led him to being reprimanded by his superiors for divulging the information that was not meant to be released. By refusing to be recorded and offered to have notes taken, it would save his job even if the superiors discover something that is not intended for sharing with non-employees of the organization. This is because even if the recording happens to be summoned back to the organisation, he will not be heard and his employment will be safe. He offered to avail himself

with the researcher as long as possible. This interview lasted over an hour and he voluntarily offered to avail himself again when needed.

Considering that document analysis had to be conducted, the researcher looked at the available legislative frameworks and documented policies in relation to digital storage where the CIOs were asked for clarity. This gave an idea of the situation the records of public sector were managed at the time of this study.

Table 4.1 Anonymised participants and roles

Participants	Role
Participant A	Record practitioner
Participant B	Record practitioner
Respondent C	Record practitioner
Respondent D	Record practitioner
Respondent E	Record practitioner
Respondent F	Record practitioner
Respondent G	CIO
Respondent H	CIO
Respondent I	CIO
Respondent J	CIO

4.2.1 Policies and legislative frameworks used for e-government services

This first objective of the study analysed policies and legislative frameworks used for cloud storage in order to support e-government services in the public sector. A lifecycle approach to the management of digital materials enables successful curation and long-term preservation, which should be performed within the ambit of legislation. The DCC Lifecycle model underpinning this study should be informed by the legislative framework with an intention to legally protect online information. Regulations enhancing robust governance structures that promote transparency and accountability must be established in order to mitigate a lawless environment when using cloud storage. In this objective, the researcher wanted to know the various legislation and policies that have been developed for digital storage. It was again a matter of determining the influence the legislation had in managing the records. Furthermore,

this objective wanted to establish the international standards and best practices that the public sector adheres to. This was a good step to identify key legislations that have a linkage to the cloud. The participants knew the legislation, but were not sure about the role of the NARSA Act of 1996. As already indicated, the NARSA Act is the key legislation regulating record keeping in cloud storage, and the researcher probed the participants in order to establish the legislation that supports cloud storage. As mentioned in section 2.3, the Constitution of 1996 has permitted the national legislation to develop a general policy framework within which government bodies should operate in order to ensure transparency. The objective was broken down into three questions, the responses to which are discussed in sections 4.2.1.1, 4.2.1.2 and 4.2.1.3.

4.2.1.1 Standards and best practices guiding management of digital records

Digital storage must be guided by legislation and international standards of records management to ensure reliable governance. The ISO standards provided that records management entails the efficient and systematic control of records from the time they are created up to the time they are disposed of. During the interviews, the researcher started by finding out the standards and best practices the participants used in their organisations. Many responses were provided and those that were the same were grouped together and are shown in Table 4.1. In interviews conducted with the participants, the researcher wanted to find the international standards and best practice indictors on digital records. The participants from IT and registry sections indicated that they used and complied with the international standards. They went further to mention that those standards were developed by the International Council on Archives (ICA). Some participants suggested that the national policy on digitalisation of heritage resources for museum, libraries and archives must be developed. They posited that developing a policy that protects the digital records from foreign countries would be helpful in a record-keeping environment. However, Participant C disagreed and explained that the presence of ISO standards did not prove useful in the public sector because they are overlooked by the records managers. Furthermore, this participant indicated that training has not been conducted to teach users how to identify and manage records. The participant explained that:

We use the ISO standards, standards from bureau of standards. So we try and follow to the best, but it is not always done properly by records managers and users in the sense that I think records managers are not trained properly. Users are not trained properly to identifying and

managing records. The content management solution we provide adheres to the standards. The ISO and Bureau of standards are ignored.

This reflected that governance of records is at risk in the public sector. Table 4.1 presents the responses provided during the discussion.

Table 4.2 Standards and best practices guiding management of digital records.

Participant A	*We use standards of archiving: International Standard for Archival Description (ISD), Standard Authority (ISA) and Standard of Archival Institutions (ISAI). International Standard for Describing Institutions with Archival Holdings (ISDIAH), International Standard Archival Authority Record for Corporate Bodies, Persons and Families (ISAAR). These standards were created by the International Council on Archives.*
Participant B	*Develop national policy on digitalisation of heritage resources for museum, libraries and archives. Develop policies that protect digital records from being owned by outsiders. There have been major invention by external funders of collection, but just because they take ownership of the records, that has been stopped. For instance, USA has laws claiming any information that has been originated by her companies even outside borders. NARSSA has not digitised with USA.*
Participant C	*We use the ISO standards, standards from bureaux of standards. So we try and follow to the best, but it is not always done properly by records managers and users in the sense that I think records managers are not trained properly. Users are not trained properly to identifying and managing records. The content management solution we provide adheres to the standards. The ISO and Bureaux of standards are ignored.*
Participant H	*No, I do not know the standards and best practices. I am not planning to do anything in relation to the digital records or digital storage. No standards. I do not have my focus on records management. Digital records is not taking place in the department.*
Participant J	*We adhere to NARSSA, ISO standards and DOD standards*

The researcher identified that the participants required the development of national policy on the digitalisation of archival resources. This became clearer when other participants confirmed that cloud storage did not exist in their department due to a lack of standards in relation to the

digital environment. Furthermore, a participant holding a senior management position in the Logistics section where registry is situated, indicated minimal interest in the functions of registry. This response as indicated in Table 4.1 clearly confirmed that the government is at risk of remaining stagnant and negating the international standards of record keeping. This is based on the fact that a manager should be in charge of the section and its legislative framework. According to the organogram of the organisation, Participant H is the head of Registry and should be in charge of the standards applicable in that section. However, the participants told the researcher that she/he did not have a focus on the standards.

4.2.1.2 Legislations governing cloud storage

Digital storage should be informed by the cloud legislation to allay fears of loss of information when the public sector considers migrating records to the cloud. Legislation refers to the laying down of instructions to the persons responsible for running a government in order to properly discharge each function of government. As discussed in paragraph 2.3.1, archival legislation provides the essential framework that enables national records and archive services to operate with authority in its dealings with other organs of state. The researcher wanted to know the legislation used for cloud storage. As showed in Table 4.2, the NARSA Act was the key legislation in this regard. On the other hand, some participants indicated that they were not governing storage according to a legislation. Some participants again reflected their negation of legislation and confirmed that their core focus is not directed to Registry. They indicated that despite the fact that registry falls within the Directorate of Logistics, they did not have a focus on it. Registry was disowned by the managers who headed it. Under normal circumstances, the Registry section should be recognised just like any other directorate, for example, Finance, Human Resources Management and many more within government. The Registry section carries footprints of the entire organisation. Giving it recognition will also lead to the provision of the necessary resources.

Table 4.3 Legislation that was used to govern cloud storage in organisations

Participant A	*We do not govern it according to a legislation. We have directives that we apply, we issue directives. The basic rule is that you migrate records to keep it readable over time.*
Participant H	*I do not know the legislations. Records management is not my core focus, it is just one other function within my directorate, but it is not really my focus, even if it falls within logistical services, I do not focus on it.*
Participant J	*Currently, we do not have a specific legislation for cloud, but there are various pieces of legislations that are applicable like ECT Act (it has provisions on how you manage digital records/data), the NARSA itself has some bearing on how your records must be managed. There is a provision that says records must not leave the National Archives, meaning that once the record has been declared and handed over to the archive, it must not leave the archive. This provision has a negative bearing on how you approach the cloud adoption. Other legislations like POPI ACT, PAIA, ECT of 2002. Ideally, as a council we need to get to a point where we develop some legislation about cloud. So you have to read the bits and pieces of legislations to make clear way on how to approach the cloud issue. If you look at SITA Act, there are mandatory services from SITA like networks. Now SITA is implementing the government cloud, which means we are now forced to use SITA cloud. Therefore, you need to read various pieces of legislation in order to come up with a business case for your environment.*

According to some participants, the NARSA Act of 1996 was promulgated for paper-based records. It was viewed as an outdated law for the cloud storage. The participants agreed that the Act supported digital records in conditions where those records are in devices like computers and servers that are securely stored on the government premises. The participants indicated that the use of cloud services, such as email hosting, were taking place without the support of legislation. Instead, Participant J confirmed that there is no specific legislation for cloud storage. However, one needs to review a plethora of pieces of legislation in order to come up with a business case for your environment.

Furthermore, the researcher wanted to know about the guidelines and policies used for cloud storage. The participants explained that there were no guidelines. Some indicated that in line

with the NARSA Act, digital records are stored on the computers, servers and many more computer devices that are locked in the government premises. On the other hand, some participants holding senior management positions in the IT environment pointed out that the government implements systems before developing guidelines, while other organisations have guidelines in place before systems are implemented. This is considered trial and error. Some participants clarified that NARSSA has guidelines on digital records; however, the Act is outdated. This comes from the fact that all digital records are kept on the premises due to the absence of specific guidelines. Some pieces of legislation that participants indicated adhering to are PAIA, POPI, ECT and DOD Act.

The researcher went further to ask the participants about the policies on digital storage. As indicated in Chapter Two, the policy on records management must correlate with the NARSA Act of 1996 in order to ensure that records meet compliance. According to the majority of participants, digital policies did not exist. However, digital records were available on the on-premises servers, computers and other devices, but they were unstructured. This ostensibly showed that digitalisation was in progress, but without policies. In agreement, Higgins (2011:79) suggests that the absence of policies that regulate the storage of records in the cloud leaves government departments to put away hard copies in an inaccessible storage with only few authorised users to ensure that it retains its integrity and authenticity. Some respondents even stated that this is caused by the newness of the digital environment in the public sector. However, some participants suggested the availability of policy, but those policies were incorrect and misleading. This can be attributed to the advent of technology that has found that people are still holding on to their old practices. Normally, transformation is difficult to adapt. It sometimes takes longer to embrace new changes. The developed digital policies can be ignored for several times before they are implemented when conducting business. The verbatim comment of the participant indicated that:

There is a policy in place, a document management policy and the records management policy in the company. The policies are adhered to, but they are not 100% right. Like in this instance, the record is given to the departmental manager to manage it, instead of registry or records manager to take control of it. The policy is there, but not right. They have written the policy, but the policy is not right. The policy says hand over the record to the manager, the manager is not a departmental records manager. They are adhering to the policy, but the policy is wrong.

Leadership plays an important role in influencing change in the organisation. Leaders must lead by examples in order to bring the new beginnings. Applying rules from top to bottom makes it easy for the junior staff to change quickly. However, that is contrary to the participating manager from records management section. The participant indicated that they did not have a focus on the legislation for cloud storage. This is despite holding senior positions in records management sections. Under normal circumstances, senior managers should know much about the sections they manage. On the contrary, the participant indicated that:
I do not know the legislations. Records management is not my core focus, it is just one other function within my directorate, but it is not really my focus, even if it falls within logistical services, I do not focus on it.

This is in agreement with the findings of Ngoepe (2012) that established that officials in Registry are marginalised. Furthermore, the *Daily Mavericks* (1 May 2019) reported that the appointment deepened the perception of the DAC as a dumping ground for under-performing senior officials (De Vos 2013). This response on its own has a bearing on records management. This study analysed NARSSA (No. 43 of 1996), which stipulates that records should be digitally stored on the servers and other storage devices which are safely locked in the government premises, which can be regarded a temporary solution. This is in line with the national archives which has a mandate to preserve and make records accessible, including those that are generated electronically. As indicated in Chapter Two of this study, Section 13(2)(b)(ii) and Section 13(2)(b) (iii) of the NARSSA (No. 43 of 1996), the national archivist shall determine the conditions subject to which digital records shall be managed and records may be reproduced electronically. In this way, the cloud storage is not provisioned. Ngoepe (2017) pointed out that NARSSA requires government bodies to migrate e-records through hardware and software changes in order to ensure that they remain accessible.

4.2.1.3 E-government services provided by the public sector

The researcher was also interested in e-government services provided by their organisations. According to Carter and Bélanger (2005:5), the primary function of e-government is to increase the convenience and accessibility of government services to citizens and to promote cost-effective government. Wahsh and Dhillon (2015) postulate that in the context of public administration, the cloud computing storage appears to be one of the most economical means

to provide e-government services towards ensuring efficiency, effectiveness, transparency, interoperability, cooperation, sharing and security, and to drive the transition to a public service of the 21st century, focused on citizen needs. The participants understood the functionalities of e-government services. They recognised the convenience and efficiency that e-government brought to the public. Some participants indicated that e-government increases access and preservation. Hu et al (2011) concur that the contribution of cloud storage to e-government services has the potential to merge distance and space, as well as reduce time, which makes the transactions of public service more effective. Unfortunately, very few participants indicated that their organisations provided e-government services. Such responses showed that the public sector was not taking advantage of using technology to provide services to the public. Their responses disagreed when Bouaziz (2008:12) postulate that the popular roles of e-government services are to enable interaction between government and citizens (G2C) and to allow inter-agency relationship (G2G). Hashemi et al (2013) held that the effectiveness of e-government services is reliant on the successful implementation of cloud storage. Table 4.3 shows the responses on the role of e-government services.

Table 4.4 Role of digital records in e-government

Participant B	*To improve convenience to public and researchers. It is the memory of the world.*
Participant D	*To create formal structure, regulate, utilisation and disposal of records.*
Participant G	*To improve or enhance on the efficiency and effectiveness of service delivery in the public sector, and also to promote and improve broad stakeholders' contribution to national and community development as well as deepen the government process.*
Participant I	*I can refer you to something I once read, somebody said if you can't google it, it doesn't exist. For the NA or any organisation to be relevant, information about that organisation must be available online. There's a huge role for digital records in e-government.*
Participant J	*The role is not only preservation. ,1. It is for purposes of preservation, 2. Preservation is done with a purpose of access. If you look within the constitutional imperatives, "whatever information that is in the government, it must be accessible to the public". So you do preservation for purposes of access and administration and information must be readily accessible when needed. South Africa is a signatory of open government initiatives, at some stage we will embark on some open data,*

	to say that government data must be accessible to the citizens to make economic value, innovation and research purposes. Kenya has a dedicated government data portal where you find government data for reuse, academic research or innovation purposes.

Cloud is crucial in the functioning of e-government services. Some of the participating records practitioners were conversant with the role cloud storage plays in the e-government. They displayed the betterment that cloud could bring to the field of records management services. The participants indicated that e-government creates memory of the world because once it is in the cloud, everyone can access it. Participant I stated that:

I can refer you to something I once read, somebody said if you can't google it, it doesn't exist. For the National Archive or any organisation to be relevant, information about that organisation must be available online. There's a huge role for digital records in e-government.

4.2.2 Public sector's trust on records in the cloud storage

As indicated in paragraph 2.4, cloud storage contributes to the enhancement of access to cloud resources. This second objective of the study was a step towards determining if the public sector entrusts records in the cloud storage. Given the long upheld paper-based storage of records on government premises, this objective was meant to assess their confidence in having their records digitised and stored virtually off campus. The concept "storage" was derived from the DCC Lifecycle model which guides how records are stored in the digital storage. Their responses would provide the direction about where they are standing with regard to migration to the cloud. Sarkar and Kumar (2016) add that cloud storage has potential means to simplify the ways of accessing e-government services between G2G and G2C. It advances time productivity amongst civil servants. The researcher had various questions to that will be listed below.

4.2.2.1 Storage of digital records and cloud

The researcher asked the participants to explain where they stored digital records. The participants explained that digital records are stored on external hard drives, on-premises servers, flash disc, and servers which are kept in a strong room. Some participants mentioned that there is not a digital policy in place. Some cautioned that there is not even a structured way

of storing digital records on the servers and computers. The participants were concerned about whether those records would be accessible or relevant in the future given the rapid speed of technology. There was fear of cloud storage because participants were not sure if the service provider could be an enemy of the superpowers. This means in the event the superpower takes a military action, information will be caught up in the crossfire. Another participant holding a middle management position in the registry indicated that records were scanned and uploaded to the system which only the service provider had access to. The same participant was worried what would happen in the event that private company is liquidated. They felt imposed to kept records with the private service provider. Within the same organisation, the participants from a different registry section indicated that they only keep paper-based records.

This was supported by the participant from the IT section who indicated that the lack of a properly structured records management section led to the duplication of records management sections. Responses of keeping records on the premises disagreed with Paquette et al (2010:247) who indicated that the former president of United State America, Barak Obama, stated that cloud computing would open up the government to its citizens. This is driven by the fact that paper-based and local storage restricts access to records. However, the participants explained that cloud can be considered, provided the legislation has been promulgated. The participants were less confident in a cloud owned by a private company. Some participants indicated their willingness to store their personal records on a privately owned cloud, but not work-related records. Table 4.3 provides responses on organisations' trust of records in the cloud. During the discussion, some participants told the researcher that efforts to develop a government cloud are under way.

Table 4.5 Organisations entrust records in the cloud

Participant B	*We are very conscious of who owns the cloud. What if the owner of the cloud is an enemy of the superpowers who can bomb the country and the cloud during the war? The private companies owning the cloud can go bankrupt. We have less trust of the 3rd party. When cabinet memos land in wrong hands, there's trouble.*
Participant F	*Yes, if there is a legislation. Now we have a contract with IS who subcontracted Mimecast where emails of this department are stored on Mimecast cloud. That means we entrust our records on the cloud. Whatever is accessed via Mimecast cannot be deleted, only that is received via inbox can be deleted.*
Participant G	*I can't say yes or no, because I don't know how the department reached an agreement with the current service provider. I only comply. I was given a system to use, then they trust them. I personally do not trust people to handle my personal information. The organisation trusts the service provider and I comply.*
Participant I	*Yes, certain clouds. I've been to few conferences in Europe for few years dealing with archival matters. Many institutions around the world are moving away from cloud for various reasons 1. Costs (they feel it is cheaper to create in-house capability) 2. Some archival repositories (your records can be held hostage when you use a private cloud, e.g. you agree to pay R1 p/m, but the organisation changes to R2 p/m which you did not agree. If you refuse to pay, they keep information) 3. Bankruptcy – a private company can go bankrupt and disappear with the information. 4. Possibility of foreign governments having access to your information. Some governments' legislations force other governments to make available the information. Then it is not safe and secure. But if it is a government cloud held by SITA, our records will not be held hostage. Therefore I do not trust private clouds.*
Participant J	*Yes. The hindrances of cloud were on sovereignty, cross-border jurisdiction where in case the cloud is in Russia, we do not even know where the physical storage is. To circumvent that, government records must be in the government owned cloud. I won't have problems if it is owned by the government. When I go to the private owned cloud and that company goes under, I stand a chance to losing data that is in their possession. If the company survives and there is a legal dispute, the USA*

	laws will apply not SA. The courts of USA will have jurisdiction over the matter, not the SA. But if it is in our boarders, we will not have such issues. If we have disputes, the company will give back the records, of course with the high costs. And accepting the records back might be an issue because I do not have the equivalent storage capacity. However, what assurance do we have to prove that they don't have a copy? And I would prefer the hybrid cloud. Creating our own cloud is costly.

During the discussion, the participants showed concern about the sovereignty of cloud. The participants were not ready to risk their records to the privately owned cloud. They displayed distrust of legislation that annexes records that might be in their country, even if the records are on the premises of a South African company. Literature revealed that trust is the key element that is required in cloud services. The records practitioners must develop trust that the records are safe. The CIOs play a seminal role in closing the gaps that might expose safety of the records. Stuart and Bromage (2010) suggested that as opposed to the telephone and electronic email, the widespread coverage of web as a space embedding the cloud means there is no need to be concerned about the persons dealing with your information, but to trust. Participant J's verbatim comment stated that:

Yes. The hindrances of cloud were on sovereignty, cross-border jurisdiction where in case the cloud is in Russia, we do not even know where the physical storage is. To circumvent that, government records must be in the government owned cloud. I won't have problems if it is owned by the government. When I go to the private owned cloud and that company goes under, I stand a chance to losing data that is in their possession. If the company survives and there is a legal dispute, the USA laws will apply not SA. The courts of USA will have jurisdiction over the matter, not the SA. But if it is in our boarders, we will not have such issues. If we have disputes, the company will give back the records, of course with the high costs. And accepting the records back might be an issue because I do not have the equivalent storage capacity. However, what assurance do we have to prove that they don't have a copy? And I would prefer the hybrid cloud. Creating our own cloud is costly.

This participant further supports that they are not interested in a privately owned cloud. They need a cloud that is owned by the government. When probed further on the conditions they expected on the cloud, participants pointed out their preference to control the cloud. Some

participants suggested that terms and conditions should be decided by NARSSA because they are the custodian of government records. The researcher wanted to know the terms and conditions for storage of records in the cloud. Participant J emphasised that:
Intellectual property of the government remains property of the government. Any record we take there, remains the record of the government. Assurance in issues of security, cyber security measures to protect whatever we put in the cloud.

4.2.2.2 Security and access to records

Digital storage propels easy access to records on the cloud. Before migrating to the digital environment, it is crucial to consider whom it will reach, motivations of stakeholders that participated in the development and deployment suitable for the consumers. Of course, it is also necessary to determine the parameters of security for those who need access. The parameters of security should be strengthened in order to mitigate those who have nefarious motives with digital records. When the researcher wanted to know how participants would deal with security of records in the cloud, some participants thought of physical security. They wanted to ensure that anyone who has access to the digital environment is controlled. Some participants explained the classification of records according to the order of importance. There were the participants who suggested that records must be kept within the Republic of South Africa. The participants from the IT section maintained that there should be a non-disclosure agreement in order to save the organisation from the people working with the information, for example, IT technicians. Table 4.4 provides verbatim responses.

Table 4.6 Access to digital records

Participant B	*Records managers, managers, and few identified staff. The rest must make request to access the records. Archives officials have access, the general public has access.*
Participant D	*Given that it is an IT instrument, ICT and GITO must have access and manager to manage the access. Managing access means managing responsibilities, giving permissions. You manage access to everyone.*
Participant I	*Two groups of people. We should have a cloud and a cloned cloud, one cloud will have your stuff, your officials working with that information. Will have access to the information that they need. The other cloud will have information that is accessed by officials and public. The one cloud*

	will have more information than the other. The one cloud will have classified records, will tell you where the records are stored. Will have all kinds of information about the records and so forth. The public cloud will have basic information about that records. It won't have classified records. Accessibility will be restricted in one cloud and unrestricted in the other cloud. There will also be a hierarchy of who will have access to which records. There will be security level set.

When probed further about who should have access to records, participants from records management stated records officials and few identified officials. However, IT participants mentioned that IT officials must manage access given that the instruments of digital records belong to IT. Participant D explained that:

Given that it is an IT instrument, ICT and GITO must have access and manager to manage the access. Managing access means managing responsibilities, giving permissions. You manage access to everyone.

In the same vein, some participants suggested everyone must ask for permission to have access. In the contrary, one section of registry in another organisation indicated that all registry staff must have access.

4.2.3 The view of the public sector on digital preservation of records in the cloud

The DCC Lifecycle model provided that preservation should ensure that material remains authentic, reliable and usable while maintaining its integrity. In this stage, there is involvement of validation, assigning preservation metadata, assigning representation information and ensuring acceptable data structures and file formats. Currently, there are preservation methods used at the paper-based storage. The DCC Lifecycle model indicates that digital preservation is crucial within the life cycle of digital records. This third objective was necessary to determine how preservation could be handled in a digital environment. This objective solicited views from the records management and IT sections. Adu (2015) opines that digital preservation gave assurance to the right to information laws that the government would accumulate and maintain information that is authentic, verifiable and reliable. It is comprised of the digital life cycle management processes, spans and archive operations that consist of acquisition, ingest, metadata creation, storage, preservation management and access (Delaney & De Jong 2015).

This objective was crucial in analysing the public sector's view on digital preservation of records. The researcher started by asking the participant how created records are preserved for the future.

Given the prominence of paper-based preservation in the public sector, most participants from the Records Management section indicated that they used micro-film for its 500-year longevity and its resistance to being corrupted. Delaney and De Jong (2015) suggest the essence of digital policy document in the organisation's commitment to preserve digital content for future use, specifically file formats to be preserved and the level of preservation to be provided and ensure compliance with standard and best practices for responsible stewardship of digital information. The majority of the participants understood the role of preservation. The participants explained that the biggest problem emanated from the lack of preservation policy and training of staff. The participant indicated that:

I think that is one of the biggest problems. There is no plan for future preservation. Like I said previously, I don't think people are properly trained and made aware of the value of records. In their minds, they use records, make it redundant and discard it or throw it away. There is no preservation policy or plan in place. If you look at the national archives, on the other hand, the systems we are implementing ensure that their records are kept forever. So there is already preservation plan in place. If you look at ATOM, there is a specific drive on preserving the records, making sure there's backups, there's making sure there's master copies. The way we work for instance, if I take recordings, they'll take recordings as a WAV file, but normally it is too big. So they will have a preservation area where they save a WAV, they make MP3 copy of it. So what will be used is the MP3 copy. And then if there is a problem with the MP3, they'll another extract from the master file. So obviously they have preservation.

In the same breath, some participants mentioned that preservation needs a proper backup strategy. They indicated the need for digital strategy leading to the formation of a data lake. That is where people can have access to information for whatever purpose. As indicated in Table 4.6, the researcher probed further about the identified benefits of digital storage. Some participants held that it provides access to records that would never have been accessible, irrespective of location and time. Ferreira et al (2017) agree that digital preservation ensures that content in digital format remains accessible over time, reliable and authentic. Furthermore, participants explained that records should be available for the future generation. Some participants stated that digital preservation is helpful in future investigations and audits. During

the discussion, the participants indicated that digital preservation promotes instant access to information.

Table 4.7 Benefits identified on digital preservation

Participant B	*To provide access to the records that would not have been accessed. There is access irrespective of location. It should be remembered that digitisation is not preservation. Preservation includes reliability and authenticity.*
Participant C	*Well, records should be available for future generation. So if you preserve records properly, the ones that have got value, our children and their children can have the benefit of seeing the records. It benefits in securing records. You cannot lose it. There is a backup to retrieve digital records. Information is available instantly as opposed to the paper-based records that are accessible in a physical format. It is easier to exchange information.*
Participant D	*It helps us to respond to audit queries. For future utilisation. For assistance in future investigations. Analysis of trends within the organisation.*
Participant I	*If the record is digitised and available online, I can see it from where I am and conduct research without having to travel and book accommodation. If it is digitised I can do research in my home without a cost. 1. Cost. 2. Benefit records won't get damaged. 3. Bringing archives to the people and our organisation. By digitising records, you are bringing archives to the people. You can spread our heritage throughout the country because the records aren't kept in one specific location. It is now on your phone where you type few words and get everything you want. You make archives more accessible to the public*

Issues of authenticity and integrity, preservation life cycle of assets as well as attention to the interests of particular communities of practice such as archivists, have major areas of interest for the DCC. The researcher was also interested in finding out about the management requirements concerning authenticity and security of digitally preserved records. The participants explained that authenticity and security are important even in the paper environment. Some participants indicated that they did not have the support of senior management in this area. This response concurred with senior records managers who indicated

that records management is not their core function. Training should be provided to records officials in order to ensure that records are handled by experienced officials. Some participants emphasised that issues of confidentiality, integrity and authenticity should not be compromised. However, other participants suggested that records should be the way they are. Participant C indicated that:

Very much. One of the problems with the digital records is if they are digital, they forget that if you get someone who knows about the records can alter the authenticity and create them as if, wow for fraudulent reasons or any bad reason. So to make sure that electronic records are authentic, you need to make that security is on par. If you have proper records management system or policy in place to manage digital records, they should be authentic on time

Delaney and De Jong (2015) concur that when changes have been made to digital records, documentation must be made, detectible and manageable to prove the changes. The investigator wanted to know the necessity to have a management requirement concerning authenticity and security of digitally preserved records. The following answers were given as indicated in Table 4.7 in relation to the discussion on authenticity and security of digitally preserved records.

Table 4.8 Authenticity and security of digitally preserved records

Participant B	*Even in the paper environment, authenticity and security are significant. Records must not be tempered with. They must not be accessed willy-nilly. Safeguard the authenticity, security for the posterity through preservation.*
Participant C	*Very much. One of the problems with the digital records is if they are digital, they forget that if you get someone who knows about the records can alter the authenticity and create them as if, wow for fraudulent reasons or any bad reason. So, to make sure that electronic records are authentic, you need to make sure that security is on par. If you have proper records management system or policy in place to manage digital records, they should be authentic on time.*
Participant D	*Yes, security-wise it means who accesses it. When did he access it? When the changes were made, what was changed and what was a value before.*
Participant E	*Yes. We need support of top management. Records management have not enjoyed support from top management. They should provide training.*

	Provide budget. Management should get involved in getting NARSSA officials to come and provide awareness.

When probed further about the ways to improve digital preservation of records, the participants were not hesitant to point at the development of policies and guidelines on digital preservation. Other participants suggested that as soon as digital preservation is in place, information becomes available for reuse. It is necessary to identify and train officials who will prove such services. In order to have improved digital preservation, a cyber-security strategy should be in place.

4.2.4 Disposal of records in the cloud

The DCC Lifecycle model prescribes that this occasional action involves the disposal of data that have not been selected for long-term preservation in accordance with the policies and other legal requirements. As opposed to the paper-based records environment, this objective wanted to assess how disposal can be applied in the digital space. It would also give an idea of whether disposal is influenced by space or regulations. The researcher wanted to know the process followed to dispose of records. NARSSA participants stated that documents that reach their premises are not disposed of in the form of destruction, because they are stored on behalf of the nation. The historical records were there for a permanent stay. They further stated that all government departments seek disposal authority from the National Archivist. However, other participants from Registry mentioned that the disposal process must not differ from current paper-based disposal where all major key role players from NARSSA are involved. Some participants told the researcher that they have a system in place that reflects the records that are due for disposal, which sends an email that informs NARSSA. When probed further, participants from IT explained that disposal was informed by a lack of space. It will not be easy to dispose of records in cloud storage because of its elasticity. As reflected in Table 4.7, Participant J indicated that:

Internet does not forget. I'm not sure if the disposal of digital records will be easy. Electronic records such as email, those are digital records. I am of the view that the disposal of records on the digital space might not be applicable. The NA act must be changed because it was written for paper-based records. Things are difficult in a digital environment. Remember that disposal was informed of space. In an online environment there is enough space which will not encourage disposal. There is interconnectedness, ICT will ensure that there's more than

enough space. Storage will always become cheaper in the cloud. The cloud service providers are killing the normal service providers of storage. Individually, you are storing data on free cloud storage. Deliberately they will make cloud come for free, this means server market will be reduced and only CSP will buy them.

Franks (2013) disagrees with the response by stating that the primary purpose of records retention and disposition is to ensure that records are retained only for as long as necessary and then disposed of when they no longer have value. A particular way should be established to dispose of digital records.

Table 4.9 Authenticity and security of digitally preserved records

Participant B	*Historical records are here to stay. No need to destroy them. However, the government departments seek permission from NARSSA to dispose records.*
Participant C	*There is a disposal authority on the system. So the system will warn the records manager that there is a record to be disposed of. Disposal has two components: destroy it or transfer it. If it is destroying, you need authority from NARSSA to destroy it. The system does that. It sends a request and it gets an answer, email to NARSSA with a file number. You put the disposal number and the system will destroy. Disposal of all e-records must be approved by NA. We follow that law. We follow the policy of not destroying a lot.*
Participant E	*The procedure should be similar to paper-based practice. The national archivist must be involved.*
Participant J	*Internet does not forget. I'm not sure if the disposal of digital records will be easy. Electronic records such as email; those are digital records. I am of the view that the disposal of records on the digital space might not be applicable. The NA act must be changed because it was written for paper-based records. Things are difficult in a digital environment. Remember that disposal was informed of space. In an online environment there is enough space which will not encourage disposal. There is interconnectedness, ICT will ensure that there's more than enough space. Storage will always become cheaper in the cloud. The cloud service providers are killing the normal service providers of storage. Individually, you are storing data on free cloud storage. Deliberately they will make*

	cloud come for free, this means server market will be reduced and only CSP will buy them.

The researcher then attempted to establish how the organisations determined the readiness of digital records that are due for disposal. Only the participants that had systems in place told the researcher that the rules reminding them about disposal have been set on the folders. On the other hand, the participants from registry stated that the age of records is a determining factor for disposal. According to Participant E,

There is a file plan developed by DAC. The provision has been stated that the record should be disposed of after some time. Ours does not show when records should be disposed. On e-records, the system should show that the record is ready for disposal.

All these practices were in line with the NARSA Act. However, the security cluster departments do not transfer to the archives, they have their own rules. Attempts to interview the security cluster departments did not yield any appointment. When the researcher probed participants about their involvement in the disposal, the participants from archives indicated that their role is to issue disposal authority to the departments. Some participants from other organisations indicated that they do verification.

The researcher also asked the participants about the disposal committees in their organisations. The majority of participants indicated the need for a disposal committee so that good decisions on disposal are taken. They felt that the current way, where in other organisations, only one official is used, is not really conducive to records management. Ngoepe (2012) agrees that as outlined in the King Report iii, every business should have an information committee of senior executives who audits the information processes and monitors the full life cycle of information – from creation or receipt to disposal. This leads organisations to become more accountable for the way in which they dispose of their records. In the same breath, some participants told the researcher that a digital officer is sufficient to look after the disposal according to the digital policy. However, Participant B explained that a disposal committee is not necessary, there should be a disposal unit within the organisation to look after the disposal. The participant further explained that there is uncertainty about how that should work and suggested that research should be conducted in order to establish how that can work. The verbatim comment of the Participant B indicated that:

The disposal committee is not necessary, but a section that deals with disposal. I am not sure how it can work, but investigation is required.

Participant J echoed these sentiments, explaining that it should not be called a disposal committee. The participant elaborated that committees have the potential of destroying other committees. Table 4.9 provides responses in relation to the formation of a disposal committee of digital records.

Table 4.10 Disposal committee of digital records

Participant B	*The disposal committee is not necessary, but a section that deals with disposal. I am not sure how it can work, but investigation is required.*
Participant E	*Disposal is a big thing. The committee shall oversee that the disposal process is run correctly. They will see if we have received authority from DAC, written approval from the national archivist. The committee will see that no one takes anything from wat needs to be disposed*
Participant F	*Yes, there must also be a digital officer to determine records policy according to the policy.*
Participant I	*We have a section called records management section. It is not a committee, but a sub-committee dealing with disposal of records. If we were not NARSSA, I would say "yes" disposal committee would add value. The sub-directorate makes a recommendation, which needs to be approved by the national archivist, who then refers it to National archives advisory council, before a final decision is taken. It is not a question of one person making decisions, firstly, sub-directorate as a whole. There is a system in place.*
Participant J	*You might need it. Let us not call it disposal committee. When you digitise paper records, you need digitisation committee. You need a digitisation committee. The digitisation committee can play a disposal committee role as well, because have many committees kills a lot of committees. The digitisation committee can play a disposal committee role as well to avoid having many committees. The role of the digitisation committee is that when you embark on a digitisation project, you prioritise. The digitisation committee will decide which one needs priority. This committee will be aware of what has been digitised, born digital, then they will make*

	decision around disposal. When we did our benchmark in France in many entities.

4.2.5 Framework for curation of records in the cloud in South Africa

The investigator wanted to know if the participants were familiar with other models that can be applied in the digital environment. The participants were not familiar with the models, citing that cloud is a new concept. When the researcher probed them further to find out if they would prefer a new or existing model, the participants indicated that they preferred to use the existing models used by other organisations. However, others suggested that a model should be useful for the current archiving environment. Even if it is an existing model, it should be customised for the archives regulations. Others went as far as stating that the recommendations of the International Council on Archives should be considered. Given that records are managed in the registry and the cloud storage is computer based, the investigator wanted to know their suggestion of prior knowledge that digital records officials should possess in order to use or understand the services of storage models. Most of the participants indicated that the prospective records officials should be computer literate. They suggested that officials must not just know the record, but also its genesis and the possible preservation method for the records. According to Participant J,

ICT skills. Curriculum needs to change. People need to be taught about how do you archive, digitise. We need people with digitisation skills, how do you take care of digitised format because some are audio, film, music, paper-based. New records worker will require digitisation skills to be able to manage records. They must learn 30% of paper-based records and 70% digital. For instance, at the national archive we have implemented the NERS system, but they don't have the system administrator. System administrators must have archival training.

Again on prior knowledge, other participants postulated that registry and IT sections should be merged in order to enhance working relationship. Working together would simplify the way in which records management is practised. Some participants held that a future records manager should possess a degree in information science and IT. This view was supported by Participant F who pointed out that:

You need a hybrid in the form of archivist and IT specialist. IT degree, Information background and IT background.

On the professional capacity required to support digital records, Participant B explained that:
They must possess photographic background in order to understand the density of records/archives. We need archivists that can describe records. We need IT-skilled officials. The officials must understand business cases. Currently, they have basic requirements of digitisation.

This is caused by the fact that records management requires various skills. In support of Participant B, Participant J stated that:
We need editors, those who understand maps, GIS skills. We have living heritage, for example, Old people who can teach you about old things. That footage becomes a record and needs to be placed on GIS. Those who understand special printers.

4.3 Summary

This chapter presented data collected from semi-structured interviews and content analysis. The target population came from Records Management and IT sections. The responses were grouped according to the themes which were classified according to the objectives of the study. The actual words of the interviewed participants were used to express the ideas as they were said. Below is a summary of key issues that were raised by the participants.

4.3.1 Policies and legislative frameworks used for records storage in the cloud in order to support e-government services:

- Lack of legislations for cloud storage
- Non-compliance with the ISO standards
- Following wrong policies
- There is no specific legislation for cloud storage, one has to read various pieces of legislation in order to come up with cloud
- The participants mentioned that they used international standards of archiving
- Some participants disagreed that the presence of ISO did not prove useful because they were not followed
- Policies are followed but they are not 100% correct

- Many of the participants mentioned that they were not providing e-government services
- Some participants indicated that they did not have their focus on records management

4.3.2 Determine if the public sector entrusts records to the cloud storage:

- The participants indicated that their records are stored on the on-premises servers, external hard drives and computer devices that are locked in the strong room.
- More than one registry section
- Develop a government-owned cloud
- They pointed out that cloud storage can be considered, provided legislation on cloud has been promulgated.
- They stated that they preferred to stored personal records in a private cloud, but not work-related records.
- They stated that they are not interested in storing records in a privately owned cloud, but in a cloud owned by the government.

4.3.3 Analyse the public sector's view on digital preservation of records;

- Participants stated that the biggest problem emanated from the lack of digital preservation policy and training of staff.
- There is a need for digital strategy leading to the formation of a data lake and reuse of information.
- Lack of support by senior management.

4.3.4 Determine the processes followed to dispose records in the cloud storage:

- Necessity to dispose records in the cloud storage.
- Formation of disposal and digitalisation committee.
- Disposal process must not differ from paper-based disposal of records where major key role players from NARSSA are involved.
- Disposal was informed by the lack of space; it will not be necessary to dispose of records in cloud storage because there will be enough space.
- Limited space in the archival holdings.
- It is not necessary to have a disposal committee, but a disposal unit within the organisation, because committees destroy other committees.
- Certainty must be reached on how the disposal unit should work.

4.3.5 Propose a framework that guides storage of records in the cloud in South Africa.

- Even if the existing model is used, it should be customised for archiving.
- The curriculum must be changed to ensure that prospective records officials possess information sciences and IT degrees.
- Registry and IT must be merged to enhance working relations.

Given the presentation above, there is an opportunity to review the current method followed to store records. The next chapter provides interpretation and discussion of findings.

CHAPTER FIVE

INTERPRETATION AND DISCUSSION OF FINDINGS

5.1 Introduction

The previous chapter presented and analysed the results of data obtained through semi-structured interviews and document analysis. As already briefly indicated in Chapter Three, the thematic analysis is employed as an analytic tool. Thematic analysis undertakes to explore, in great detail, core common features in textual data in order to make sense of the meanings found in the data (Braun & Clarke 2006). Given the qualitative nature of the present study, data were generated from semi-structured interviews held with records management officials and CIOs from various government departments. This chapter provides the interpretation and discussion of findings.

According to Neuman (2011:177), interpreting data means to assign significant or coherent meaning to the results. This process comprises preparing data analysis, moving deeper into comprehending the data and making an interpretation of the bigger meaning of data. In discussing the findings, some perspectives will be drawn from the constructs of the DCC Lifecycle model, the theory underpinning this study. During the discussion of findings, it is essential to evaluate and interpret implications of research problem. Babbie (2001) and Neuman (2006) remind the scholars that even if data were properly collected analysed, incorrect interpretation would lead to inaccurate inferences. To minimise that, interpretation must be done in an objective manner. Data were analysed using themes that originated from research objectives where all responses addressing a particular objective were grouped together. The results were interpreted and presented based on the following research objectives:

- Analyse policies and legislative frameworks used for records storage in the cloud in order to support e-government services
- Determine if public sector entrusts records on the cloud storage
- Analyse the public sector's view on digital preservation of records
- Determine the processes followed to dispose records in the cloud
- Propose a framework that guides storage of records on the cloud in South Africa

5.2 Policies and legislative frameworks used for e-government services

This first objective was intended to find out what legislative frameworks govern cloud storage in support of e-government in the public sector. In addressing this objective, the researcher had to analyse legislations, records-management policies and ISO standards that are used at the archival holdings. The interpretations and discussion of findings are presented in themes. It should be noted that some of these themes might not reflect in the previous chapter. This is caused by the fact that as the discussion proceeds, the information would merge and make the paragraphs duplicate each other. The following themes were generated from the first objective of this study:

- Compliance to standards and practices of digital curation of records
- Absence of legislations for cloud storage
- Lack of policy for cloud storage
- Minimal support by the senior management
- E-government services provided in the public sector
- Managers are not familiar with cloud legislation
- Unaligned policies with the practice on records management
- Lack of support by senior management on ISO standards

5.2.1 Compliance to standards and practices for digital curation of records

The ISO standards are essential in ensuring that records management of any country is in line with what happens in the world. The ISO standard provides that records management entails the efficient and systematic control of records from the time of creation up to disposal. With regard to the standards and best practices for the cloud, the participants confirmed that they use ISO standards that have been approved by the International Council on Archives. Indeed, South Africa has adopted ISO standards for the records management, such as ISD, ISA, ISAI. ISDIAH, ISAAR and many more standards created by the International Council on Archives. This was confirmed by the participants who agreed that they use international standards of archiving. This goes hand in hand with the DCC Lifecycle model because it guides the life cycle of records management. The standards ensure that the organisations have the proper guidelines when embarking on digital curation of records. As opposed to what other participants observed about the use of ISO standards, this study revealed that officials do not

adhere to the ISO standards. One participant argued that the availability of ISO standards do not prove useful, because they are not properly followed. In principle, overlooking standards is tantamount to ignoring the rules and procedures of how records should be handled. That might attract the cyber-attacks when cloud users do not adhere to the standards. It might negatively impact the sequence in which records are expected to be stored in the cloud. The participant attributed this to the lack of training of records management officials in how to identify records and their value. This finding is echoed by the participant heading the Logistical Services section, where Registry forms part of the directorate, who mentioned that she is not planning to do anything about registry because she does not have a focus on it. Training creates awareness of how to apply the standards to the records and understand the value they bring to the organisation. On the other hand, Franks (2013) propounds that an effective records management programme comprises records management policy and procedures, well-trained personnel, advanced information systems and reduced risks within the records management environment.

5.2.2 Absence of legislations for cloud storage

Mittal (1971:4) describes legislation as the laying down of instructions to the persons responsible for running a government in order to properly discharge each function of government. Ngoepe and Saurombe (2016) postulate that legislation has a huge impact on how records are stored in any country. However, the research findings of this study revealed that the government departments do not have a specific legislation that governs cloud storage. In the absence of cloud legislation, the participants from the IT environment explained that one needs to read various pieces of legislation in order to come up with cloud information. The participants agreed and indicated that government is reliant on NARSSA No 43 of 1996 to regulate records management matters. However, some participants held that the NARSSA is outdated, because, as indicated in Chapter Two, it only supports paper-based storage where records are securely locked in the government premises.

In this case, the records are available to those who can visit the premises where they are stored. This causes contradiction to the South African Constitution that provides that the national legislation should establish the general policy framework in terms of which governmental bodies should operate to ensure effectiveness and efficiency of information. The participants believed that the NARSA Act has bearing on cloud storage, because relocation to virtual space

is involved. The participants propounded that reliance on NARSSA is a hindrance to records keeping rather than providing a solution to cloud adoption of cloud. This is also fuelled by the provision that all records moved to the archives must not be shifted from the government holdings. Indeed, migration to the cloud leads to the digitalisation and migration of records to the virtual storage, which is managed by the CSP. Being in that space, access becomes ubiquitous and accessible from anywhere at any time. Despite the fact that the NARSA Act supports digital records and digital storage, it refers to servers and other computer devices that are securely locked in the government premises. The reliance on the NARSA Act might be that it served the purpose of having all records on government premises because they were stored manually. In support of this view, Ngoepe and Saurombe (2016) opine that the Act was drafted with paper records in mind. On a positive note, paper-based storage paves the way to a well-organised manner that will simplify digitalisation because records will be categorised according to their value as they embark on migration to the cloud. Having cloud legislation drafted and enacted would allay fears that government departments have and benefit community with regulated online access of records at their convenience time. As identified and confirmed by the participants, the NARSSA is at this point not fulling role where e-government services could be attained.

5.2.3 Lack of policy for cloud storage

This theme is an expansion of the above-mentioned theme, however, it is necessary to have its standing subheading in order to minimise confusion to the readers of this this study. The International Council on Archives (2005) defined policy as mandating practices within a specific individual organisation or group of related government or organisations. According to Franks (2013), effective records management programme comprises records management policy and procedures, well-trained personnel, and advanced information systems which reduce the risks within the records management environment. On the contrary, this study reveals that despite the availability of unstructured digital records on computer devices, there are no policies and guidelines in place. Ngoepe (2012) views that failing to implement records management policy, governmental bodies will not be able to meet the obligations required of them. However, some participants indicated that government departments implement systems before developing regulatory framework. This sounded unfamiliar, because implementation is driven by policies and guidelines.

This study further revealed that some public sectors adhere to incorrect policies. This was confirmed by the participant who pointed out that policies have been developed, but are unaligned with the way in which records should be managed. According to the participant, the policies are adhered to, but they are not 100% right. For example, the records are handed over to the departmental manager instead of the records manager. The departmental manager does not have knowledge of how records should be handled. Therefore, it means the organisation is following incorrect policies. In contradiction, NARSSA (2007) provides that in South Africa, the current records management policies promulgated by the public archivists support the role performed by all these players in the creation, management, identification and preservation of information sources. While conducting content analysis on the record-management policies provided by the participants, the content was similar despite the different titles. In them, digital curation or digital storage referred to the computer-related devices such as servers, external hard drives that are kept on the government premises. Nowhere cloud storage was mentioned in all the policies. Furthermore, the policies were influenced by the NARSSA.

In addition to policies, this study revealed that the NARSA Act contains guidelines for digital records; however, the participants were not aware of them. This was confirmed by the participants from the IT environment who indicated that government departments implement before developing policies and guidelines. This clearly confirms the concern raised by participants from the Records Management section who indicated a lack of training in and awareness of the records and policies. However, given that cloud storage for record keeping has not been adopted, there are no guidelines for cloud storage. In contrast to normal practice where policies and guidelines are developed, the participant pointed out that the standards are developed after the implementation has taken place.

5.2.4 Minimal support by the senior management

Managers should be involved in the governance frameworks of the organisations. It emerged in this study that senior managers are not interested in knowing legislations that has anything to do with the cloud. This was confirmed by the participant holding a senior management position who indicated that cloud legislation or cloud policy does not exist. The participant also mentioned that is not her core focus. According to the participant, registry is just one of the functions in her directorate, but she does not focus on it. This finding proves that the records management section is marginalised and managed by managers who are not passionate about

records management. In a study by Ngoepe (2012), it was confirmed that registry is marginalised and managed by unqualified officials. Being the head of the directorate, this participant was expected to be the main driver towards the implementation of all legislative governance frameworks of records management in the organisation. Under a well-functioning organisation, the Director: Logistics is responsible for the legislative framework records keeping. The registry section reports to or is headed by this senior manager. The legal documents in the form of policies, standards and procedures become her responsibility.

Coupled with these findings, the *Daily Mavericks* (1 May 2019) reported that marginalisation begins at the appointment of political heads in the Department of Arts and Culture (DAC) to which the Records Management division, NARSSA, reports. The newspaper indicated that the appointment deepened the perception of the DAC as a dumping ground for under-performing or politically radioactive ministers of a ruling party and that has extended to the Registries in government departments. When Minister Nathi Mthethwa was appointed to the role of Minister of Arts and Culture from the police portfolio in 2014, it was perceived to be a political demotion. The minister was embroiled in a number of political scandals, chief among them was the poor handling of Marikana Massacre. Any appointment in the DAC is viewed as a demotion, because the DAC's political capital is deemed to be low. In the same breath, the officials appointed in the registry are considered unintelligible. In stark contrast, the policy has stipulated the level of qualification that such people should have, but that is not practised. This call was made in line with section 91 (3c) of Chapter Five of the Constitution, which permits the president to make no more than two Cabinet appointments from outside the ranks of the National Assembly.

5.2.5 E-government services provided in the public sector

As already indicated in Chapter One and Chapter Two, the primary function of e-government is to increase the convenience and accessibility of government services to the citizens and to promote cost-effective government. E-government takes the government to its citizens. During the interviews, the participants, mainly the CIOs accepted the role played by the e-government towards improving services to the people. Some of the examples that came forth included tax filing provided by the South African Revenue Services and smart card ID provided by the DHA. The participants understood the functionalities of e-government services. They recognised the convenience and efficiency that e-government brought to the public. Some

participants indicated that e-government increases access and preservation. Unfortunately, very few participants indicated that their organisations provided e-government services. Such responses showed that the public sector was not taking advantage of using technology to provide services to the public. However, the participants justified that they are not confident in taking records to the privately-owned clouds. Some of the CIOs pointed out that the government, driven by SITA should develop the infrastructure in order to attain e-government. The participants from registry sections observed that should indeed e-government, be implemented, their job would become simple. On the other hand, some were concerned that services provided through cloud computing technology would make them redundant, because they are familiar with providing services manually. However, training can get all practitioners participate confidently in the e-government. Though each participant was interviewed individually, the records practitioners and some CIOs concluded by indicating that only when the government can have a legislation or government-controlled cloud shall they consider cloud services and e-government. Rightly so, digital curation of records would also depend on the cloud legislative framework in order to fulfil the effective and efficient e-government services.

5.3 Public sector's trust on records in the cloud storage

The purpose of the second objective was to establish if the public sector entrusted records to cloud storage. In tackling this objective, the researcher was guided by the DCC Lifecycle model which underpins this study. The construct "storage" is derived from the model. Interpretations and discussions of findings of this objective are guided by the following themes:

- Storage of digital records on the premises
- Multiple registry sections
- Develop a government-owned cloud

5.3.1 Storage of digital records on the premises

The ICA of 2005 holds that the evolution of technology has led to the development of systems used for records creation and records management, which is in line with the DCC Lifecycle model. This study revealed that government departments store digital records on computer devices that are safely locked on the government premises. This creates isolation as no one except those visiting the premises have access to these records. These findings disagreed with

former president of United State America, Barak Obama, who stated that cloud computing would open up the government to its citizens (Paquette 2010:247). The participants mentioned that they are not confident to abandon the current paper-based storage because they are conscious of who owns the cloud. Ngoepe (2014) confirms that although public servants informally and unconsciously put some records in the cloud, government departments in South Africa are sceptical to entrust their data to the CSP due to a lack of trust, jurisdiction, legal implications, data privacy and security risks related to MISS. Furthermore, some participants were concerned about the retrieval of those records in the future given the fast-paced evolution of technology. This was related to the records stored on the dicta-belts that were eventually overtaken by time. The dicta-belt had to be converted in a way that would make records retrievable and readable.

The on-premises storage of records in the formats such as paper, audio and microfilm is supported by the NARSA Act. The reason might be that records management predates technology records management systems. However, today's IT network infrastructure, including telecom, cable, internet and wireless are converging into one standard governed by the cloud (Sheng et al 2012). Adopting the technology of storing records requires various skills in order to embrace it. Another reason might be that the government has not formally legislated cloud legislation. This view is confirmed by the participants who suggested that migration to the cloud can be considered if legislation has been promulgated.

5.3.2 Multiple registry sections

The findings of this study revealed that some government departments have more than one records management section performing similar functions. This is confirmed by the participants of the same organisation from different sections of records management who store records in different places. According to Ngoepe and Van der Walt (2010), decentralised registries are usually established if there would be unnecessary delays in accessing files if they were not kept near individuals working with them. One participant indicated that the records are scanned and uploaded to the system that is owned by the service provider. These records are digitally stored outside the government premises. The participant explained that their role as records management officials is to scan, upload and retrieve records while major functions on digitised records are performed by the service provider and the records owners were not even aware if there would ever be skills transfer.

Those records can only be accessed within the LAN through the system provided. Ngoepe and Van der Walt (2008) further assert that decentralised registries can give rise to inconsistent systems and records management practices, as well as duplication of files. It also requires the use of more office space and shelving, and prevents the accurate estimation of staff recruitment and training needs. The participant goes further to explain that the original copies are kept on the premises. She was concerned that the space was running out, pointing at the boxes full of files all over the floor. However, she mentioned that the organisation was in the process of sourcing a building to move the original records off campus. She admittedly confirmed that even though the premises will be privately owned by the private sector, the public sector will account for any possibilities. This participant from records management section mentioned that there are accredited landlords that can provide archival holdings to government departments.

However, there was no document to substantiate the assertion. To make it more contradictory, a three-way quotation is followed to source the building. This also shows how differently the legislation is interpreted when considering the mistrust of privately-owned cloud in favour of privately-owned buildings to store paper records while the same system cannot be applied for digitalised records. This reveals that there is a need to create uniformity on records. Against the Act, this plan again reflects that records management is obviated to look for better way for improved storage in the cloud. On the other hand, the other section keeps all records on the premises predominantly on paper and micro-film.

5.3.3 Develop a government-owned cloud

It is believed that cloud storage contributes in the enhancement of access to computing resources for enterprises interested in the development of a robust IT infrastructure in developing countries where the possibilities of doing so can be difficult (Dahiru et al 2014). However, it emerged from this study that the government does not have its own cloud. SITA has indicated to be in the process of developing a cloud that only state institutions can purchase a space. According to the participant, the cloud will be managed and kept on SITA premises. In order to have records in the cloud, a CSP has to be approached. Against that view, the participants indicated that they cannot store government records in the privately owned cloud. The participants indicated that they prefer to store records on government premises. Amongst the fears the participants mentioned with regard to such cloud storage include insecurity of records. De and Pal (2014) confirm that security is the most important technical factor that

obviates cloud adoption. This is coupled with the fact that South Africa does not have a cloud governance framework.

On the other hand, the participants holding senior positions in IT indicated that they have email services hosted by the CSP. They have entered into service level agreements on behalf of their organisations with the CSP where they are billed for their allocated space. This finding is confirmed by Shen et al (2012) who traced the conception of cloud computing back to 1961 when John McCarthy predicted while giving a speech to celebrate MIT centennial publicly, that computation may someday be organised as a public utility. This model permits cloud consumers to pay for their allocated cloud space just like household utilities like water, electricity, data and many more services.

On the other hand, participants from the records management section clearly propounded that they mistrust the CSP. Ramgovind, Eloff and Smith (2010) advise that in order to have a secure cloud computing solution, it is essential to decide on the type of cloud to be implemented between the deployment models; for example, public, private and hybrid and this role should be conducted by the IT managers or security officers. However, the participants mentioned that they store personal records instead of risking government records on the privately owned clouds, for example, Dropbox. Chihade and Van der Merwe (2017) postulate that there is a myriad of risks and challenges that every organisation should heed. The participants listed some of the following factors that form hindrances when considering migration to the cloud adoption:

- Lack of cloud legislation
- Bankruptcy of the service provider
- Enemy of superpowers
- Lack of trust of a third party
- Selling of personal information
- Hindrances of cloud were based on sovereignty
- Cross-border jurisdiction
- Loss of control over records

These factors have been confirmed by Mirashe and Kalyankar (2010) who indicate that despite the advantages in the business perspective, cloud computing also presents challenges,

particularly regarding the distrust of users to put their data on computers that they cannot control. The participants suggested that a government-owned cloud can circumvent these factors. The conditions to use cloud storage should be determined by NARSSA. The cloud should be within South African borders. Ebaid (2011:108) observes that it is difficult for organisations to avoid risks. Ngoepe (2012) agrees that what matters most are the identification and management of risks that the organisation is exposed to.

5.4 Public sector's view on digital preservation of records

The purpose of this third objective is to discuss how digital records are preserved in the cloud. In line with the purpose of study, this objective would establish how digital curation of records in the cloud to support e-government in South Africa would be achieved. This objective is addressed through the theme that was generated from Chapter Four supported by the literature reviewed in Chapter Two. The interpretations and discussions are presented through the theme of formation of a data lake:

In line with DCC Lifecycle model, which underpins this study, Higgins (2008) points out that digital preservation comprises some of the following constructs: store, access, ingest, create and preserve. Given the proliferation of technology, digital curation of records has become a necessity in record management areas. This study revealed that records managers prominently use micro-film to preserve because of its longevity of 500 years. The Canadian government (2012) espouses that various governments that started with paper-based storage of data have supported the shift to digital preservation through enacting a number of legislations and changes in policies. On the other hand, this study revealed that the available digital records are preserved on the servers and computer devices. Furthermore, due to the lack of legislation and policies from the current findings, it is clear that preservation in the cloud is not taking place, but performed on computer devices that are stored on the government premises. Rogers (2015) confirms that internal support for accountability depends on how information and records are created, managed, and preserved in order to provide for government accountability. However, preserving records and having them stored on the premises where only few people can gain access to them do not encourage openness to the public. One participant mentioned that there is no plan for future preservation. This is caused by the fact that people are not properly trained in and made aware of the value of records. For example, the participant mentioned that records are made redundant and discarded. Furthermore, the participants mentioned that there is not a

digital policy in place. They have admittedly confirmed that digitalisation takes place regardless of the absence of the policy.

Ngoepe (2017) suggests that the South African government envisions the offerings of e-government services, and has already partially realised the vision (application of identity documents, passport online, as well as filing of tax returns). It is necessary to have digital preservation in the cloud in order to support such services. This goes hand in hand with the participants who indicated that the digital strategy should be developed leading to the formation of a data lake. Data lake allows massive amounts of data to be stored in their original format. It is a storage repository that holds a vast amount of raw data in its native format until that data are needed. It is familiar with the use of a flat architecture to store data. The purpose for which data in the data lake are used for are not defined until the data are required. In the midst of data lake, NARA describes the responsibilities required to maintain the records in archival holdings as preservation and digital preservation. NARA states that preservation provides a mandate to care for the physical holdings and perform preservation by reformatting digitisation of physical items. On the other hand, digital preservation provides support for electronic records processing, perform audits of the holdings and assess the need to perform preservation action.

This is where people will have access to the information for whatever purposes. This has been evidenced by the study of Ferreira et al (2017) who confirm that digital preservation ensures that content in digital format remains accessible over time, reliable and authentic. It would be helpful in future investigations and audits. As part of the benefits, participants believe that digital preservation provides access to records that would never have been accessed, irrespective of location and time. The issues of confidentiality, integrity and authenticity should not be compromised. However, other participants suggested that records should be the way they are. This is because the ICT infrastructure has converged. This gives an advantage to the public sector to consider migrating to the cloud where preservation will provide long lasting availability of records to be accessed by the public.

5.5 Disposal of records in the cloud

This fourth objective was intended to identify how records are disposed of in cloud storage. It also has a link to the DCC Lifecycle model. The DCC Lifecycle model, which underpins this study, points out that the disposal of records forms a crucial part of records management. The

NARSA Act defines disposal as a permanent storage or destruction of records; however, it requires disposal authority. The NARSA Act stipulates that disposal authority is a written authority issued in terms of section 13(2)(a) specifying records to be transferred into the custody of the National Archives or specifying records to be otherwise disposed of. In agreement, Ngoepe and Nkwe (2018) point out that in terms of the NARSA Act, "no public records may be transferred to an archives repository, destroyed, erased or otherwise disposed of without the written authorisation of the national archivist". This objective has been discussed in the following themes:

- Necessity to dispose of records in the cloud storage
- Limited space in the archival holdings
- Formation of disposal and digitalisation committee

5.4.1 Necessity to dispose record in the cloud storage

The disposal of records stored in the cloud is not easy. The participants from the IT environment agreed that the technicalities of the cloud and its elasticity discourage disposal. The participants held that disposal was informed by lack of space. It would not be easy to dispose of records in the cloud storage due to its elasticity. This means that in the event that the storage runs out of space, a consumer can just buy extra space. In agreement, this was confirmed by the participants who argued that the internet does not forget and it proves difficult to dispose of records in the cloud. The disposal of records in the cloud environment is technically and organisationally difficult. Duranti and Jansen (2013) concur that the multi-tenancy model utilised by CSPs to reduce service costs create complications with regard to the ultimate destruction of records. This means the traditional method of wiping a disc and overwriting the sectors with random digits cannot be accomplished when other tenants are concurrently maintaining active records on the same disc. Although each consumer has been allocated space, they share similar resources whereby it proves difficult to even format a multi-shared disc, any attempt to destroy the disc can unintentionally be detrimental to other clients sharing the same space.

The participants suggested that the disposal process of digital records in the cloud storage must not differ from paper-based disposal where major key role players from NARSSA, for example the National Archivist, are involved. The previous sections have indicated that the public sector

does not store records in the cloud. Having indicated that government is still new to the cloud concept, some participants indicated that one needs to drill the hard drive in order to destroy digital records. This disposal method has its proximity to the digital records that are stored on the on-premises computer devices.

5.4.2 Limited space in the archival holding

The participants from IT environment, CIOs viewed that disposal of records in the form of permanent destruction was informed by the limited space in the archival holdings. They viewed disposal as a way of creating more storage space for the records. Franks (2013) disagreed by stating that the primary purpose of records retention and disposition is to ensure that records are retained for only as long as necessary and then disposed of when they no longer have value. On the other hand, the DCC Lifecycle model, which underpins this study, sees the life cycle of a record as a progression through distinct stages from creation to disposal.

The participants suggested that there is enough space in the cloud environment, which will discourage disposal of digital records. The inter-connectedness of ICT infrastructures ensures that the space is always available. Given the demand and necessity of a flexible model of records storage in the cloud, the participants predicted that the space will become cheaper. Moghaddam et al (2015) confirm that cloud-based services are prominent in relation to on-demand services and unlimited storages in the organisations. The findings indicated that the NARSA Act is old and must be changed because it was written for paper-based records. The participants believed that cloud storage is destroying the market of normal service providers of storage where paper-based records are kept. For example, individuals store their records without charge in the cloud environment. This expedites the lower price for the cloud storage while it also influences that the server market will be reduced and only CSPs will purchase it to create more digital storage.

5.4.3 Formation Disposal and digitalisation committee

The King report iii stipulates that every business should have an information committee of senior executives who audits the information processes and monitors the full life cycle of information from creation or receipt to disposal (Ngoepe 2012). Against the King report iii, the findings of this study revealed that the public sector does not have either a disposal committee

or a digitalisation committee. This is confirmed by the participants who opined that their reliance on a sole individual for disposal is not good for proper governance of records management. It is assumed that an individual taking a sole decision might cause the problem of disposing of what was not intended. However, there are participants who are in agreement with the formation of a disposal committee so that good decisions on disposal are not compromised. Working together as a team minimises mistakes. Another participant stated that the disposal committee is not necessary. Instead, the organisation should do away with committees and form a directorate that will concentrate on disposal matters. The participants suggested that a digitalisation committee must be formed to perform the disposal function. Normally, committees are formed and dissolved. Reflecting on the DCC Lifecycle model, the life cycle of a record is a continuous sequence. On the other hand, a directorate is sustainable because it has officials that are dedicated to their work as opposed to a committee whose members have other commitments in their respective sections they report to. A committee might be scheduled to meet once at a particular time and it is possible for the committee to meet as planned. Chances of failed meetings are high, leading to postponement of serious decisions on disposal when members cannot quorate when some members have other commitments. However, a directorate will implement activities as planned even if all the officials are not around, because everything will be going according to the plan.

Another participant echoed the same view on doing away with the disposal committee by indicating that it should not be called a digitalisation committee. The participant argued that committees have the potential to destroy other committees. Instead, the participant suggested the formation of a digitalisation committee. Such committee could be crucial in the disposal role, because it has relevant information of available records. For example, prioritisation takes centre stage when the digitalisation project is embarked on. This committee will be aware of what has been digitised in order to take decisions around disposal. Another participant suggested the formation of a disposal section. However, given the uncertainty around how that directorate should work, the participant suggested that research should be conducted to determine its functionality. Indeed, it is impractical to dictate new development without testing how it will work. Training of those who will be involved is necessary to avoid losing records. Irrespective of whether a committee or a directorate is formed, disposal of records will require more than one official to provide inputs in order to avoid disposing of what was not meant to be disposed of. In cognisance of the fact that disposal was based on limited space for paper-based records, it should also be reviewed if it should take place in the elastic cloud storage.

5.6 Summary

This chapter interpreted and discussed the findings of this study that were presented in Chapter Four. The discussion was based on the DCC Lifecycle model which underpins this study, as depicted in Chapter One and the literature reviewed in Chapter Two, in the context of previous studies. The reviewed literature was also consulted to support or argue against the findings of this study. The findings were interpreted and discussed according to the objectives as presented in Chapter One.

There was consensus amongst participants from both IT and Records Management sections that the public sector does not have specific legislation for cloud storage. The government is reliant on the NARSA Act which, according to the participants, is outdated. This is because it advocates that government records should not be shifted from the government premises. It can be argued that despite the crucial role played by the records management sections, senior managers do not have their core focus on this section. The discussions also revealed that senior managers are not even interested in knowing the legislation that guides the storage of records in the cloud. This crucial section is also considered a place for non-performing officials within the organisation.

The discussions further revealed that some public sectors are adhering to incorrect policies. They believed that the policies are not 100% right. The participant attributed this to the lack of training of records management officials in how to identify records and their value. The government departments store digital records on computer devices that are safely locked on the government premises. Some organisations have more than one records management section performing similar functions; however, they store records in different ways: some keep records on the premises while others scan and upload records to the records management system owned by the service provider.

The discussions revealed that the available digital records are preserved on servers and computer devices. Finally, the participants from the IT environment believed that the disposal of records in the form of destruction is not easy in cloud storage due to the multi-tenancy model used by the CSP and the elasticity of the cloud. The next chapter provides conclusions, a summary and recommendations of the entrusting of records to the cloud to support e-

government services in South Africa. The chapter also proposes a framework that will assist in the migration of paper records from on-premises storage to the cloud storage.

CHAPTER SIX

SUMMARY, CONCLUSIONS AND RECCOMENDATIONS

6.1 Introduction

The preceding chapter discussed the findings that were presented in Chapter Four. The current chapter revisits the research objectives of this study in order to present a summary, conclusions and recommendations based on data findings and data presentation in Chapter Four and Chapter Five. According to Leedy and Ormrod (2010:296), all loose threads are gathered together, as in the end, research must come full circle to its starting point. The current chapter is structured to include the following: a summary of the findings, conclusions according to the objectives of the study, recommendations, proposed framework and suggestions for further research. These are presented according to the objectives of the study. In addition, this chapter proposes a framework that embeds the migration of paper-based records to cloud storage. It is hoped that the proposed framework will become an enabler for the public sector to adopt cloud storage with the intention to make records accessible ubiquitously, regardless of time and location. The chapter will make suggestions on future research arising out of this study, point out the practical implications of the results and governance framework. The purpose of this study is to explore digital curation of records in the cloud to support e-government services in South Africa. The specific objectives were to:

- analyse policies and legislative frameworks used for records storage in the cloud in order to support e-government services
- determine if public sector entrusts records to the cloud storage
- analyse the public sector's view on digital preservation of records
- determine the processes followed to dispose of records in the cloud
- propose a framework that guides storage of records in the cloud in South Africa.

6.2 Summary of the findings

This section presents the summary of findings according to research objectives in order to answer research questions of this study as indicated in section 1.4.

6.2.1 Legislative frameworks and policies for cloud storage

Governance framework plays a crucial role in the digital storage of the public sector. It ensures the protection of records from being used wrongly or damaged by unwanted sources. The private sector is in the forefront with regard to providing electronic services to their clients. Through the literature review, this study established that the public sector does not have cloud legislation. To that effect, the results suggested that a myriad pieces of legislation have to be consulted and integrated in order to come up with cloud information. Based on the literature review and discussion, it is clear that not much progress in the public sector has been made regarding cloud storage. Such delay is against the prescriptions of the Constitution of South Africa which has the highest regulatory function, and stipulates that the national legislation should establish the general policy framework by which governmental bodies should operate to ensure effectiveness and efficiency of information. The absence of a legislative framework erodes confidence of the public sector to take advantage of cloud storage and discourage paper-based storage on government premises.

According to Ngoepe and Saurombe (2016), legislation has an enormous impact on how records are stored in any country. Various countries across the globe, particularly Europe, America and Asia, have progressed in developing legislative framework in order to improve the provision of e-government services to the citizens. Having seen the simplicity of the way in which the private sector provides services, the public sector would become ubiquitous to the citizens because information would be available at any time. However, it is evident from literature review that the public sector is reliant on the NARSA Act. This Act is considered outdated because it advocates that records are stored on the government premises. This Act is viewed as a document that supports who are closer or who can travel to the premises in order to gain access to the records. It again has bearing on the migration to cloud storage due to its sensitivity to the fact that government will lose control of records when records are shifted from the current environment. It hinders the adoption of cloud storage, because it prescribes that records, irrespective of their format, must not be shifted from government premises. Since the NARSA Act is silent on cloud storage, it is believed that its support for digital storage is limited to the computer devices that are kept on the government premises.

Furthermore, literature review indicates that South Africa has adopted ISO standards that are required for records management. This is a clear indication that the country has interest to apply

best practices for its footprints given that those standards have been developed by the ICA. It means that the country envisions itself to be in line with what other countries do towards advancing access to information through e-government services. Literature review adds that the ISO standards are essential in ensuring that records management of any country is in line with how other countries manage records. In the contrary, the study reveals that the available ISOs are not adhered to. This alludes to the lack of support and training of records management practitioners. It is clear from the discussion that records management officials do not get support from senior management. Even though the records management section maintains the footprints of the organisation, the officials hardly receive training. This concurs with the discussions revealing that senior managers do not know cloud legislations and that they do not have a focus on records management. Managers are expected to drive the governance framework and implementation of relevant regulations in the records management environment. As literature review reveals that the records management section is marginalised, failure to commit themselves will lead to the status quo. Again, the study reveals the understanding that managers have a records management section within their directorates, but they are not focused on it. This will create hostility between the managers and subordinates because they will carry the blame for underperforming and failing to adhere to the ISOs. Training helps officials to identify the value of records and improve in their work.

The current study reveals that policies and guidelines for digital storage and records have not been developed in the public sector. This is evidenced by the unstructured digital records that are stored on the computer devices without even a file plan. It emerged that the government embarks on implementation before the guidelines have been developed. This leaves records management officials to upload the available digital records on the computer devices just for the sake of reducing the load they have. Unstructured digital records that are not supported by the policy or guidelines will be difficult to retrieve quickly because more searching is involved. The existing policies are irrelevant because they mislead the officials within the organisation. This is realised when an official hand over a record to the departmental manager instead of records management practitioner in the records management section. It is believed that a departmental manager, who the policy dictates should receive records, does not have competency in handling records. According to Ngoepe (2012), failing to implement records management policy, governmental bodies will be vulnerable to meet the obligations required of them.

6.2.2 Entrusting public sector records in the cloud storage

The literature review indicates that the public sector stores digital records on computer devices that are safely locked on the government premises. This study revealed that the public sector is not migrating from the current paper-based storage, because it is conscious about who owns the cloud storage, particularly the privately owned cloud in the absence of cloud legislation. The discussions painted the picture that records management is isolated from citizens and the world because the records are accessed manually by visiting the storage premises. Most importantly, isolation can be attributed to the minimal trust the public sector has in the privately owned cloud. It is believed that government records cannot be entrusted to the host of private cloud due to various issues that include security, lack of legislation, lack of government cloud, minimal trust of third parties, cloud sovereignty and cross border jurisdiction. Given the examples on literature review, the banking sector has successfully created a platform where clients perform transactions online. Keeping records in the cloud will result in opening the government to the citizens through provision of e-government services. Literature review indicates that records management has been existential long before technology. This resulted in drafting regulations that govern records management in a paper-based storage. To that effect, the public sector uses the paper-based storage which has been used over the years. Adopting a cloud storage model requires various things; for example, training, legislation, converged IT infrastructure as well as management that is willing to provide information transparently, efficiently and effectively to the public.

The results indicated that some organisations within the public sector have more than one records management section. The records are stored differently from one another, for example, one section scans digitised records and have them uploaded to the records management system that is owned by the private sector. The participants in the records management section explained that the managers opted to digitally store records in digital storage owned by private sector. The records practitioners argued that they do not know what is happening to the on the other side of the private sector. Their role is to digitize and upload to the provided system. These records practitioners indicated as much as the building was full of records, they are unwilling to use this system in the absence of clear documentation from NARSSA. However, refusing to do as managers want would lead to insubordination and they might be reprimanded. They further mentioned that they have been allocated very minimal rights, for example, uploading and retrieval. They pointed out that not even the IT section of their organization had

rights. The current study established that this storage method is not cloud-based. It was confirmed by the participants by explaining these digitized records are only accessible through the LAN when they are at work or by making a request from the service provider. They said they would be confident if IT section was involved.

The another section strictly stores records on the government premises and the NARSA Act is adhered to in full because these methods are used to store records on the premises. On the other hand, literature review indicates that cloud storage is considered an effective way to store records in an easily accessible manner. This study also reveals that the only way the public sector can have records in the cloud is through contracting a CSP. This is informed by the fact that the government has not developed its own cloud. The participants indicated that a privately owned cloud is deemed relevant to store private information, for example, curriculum vitae and other personal information. The current study proposes that the government must have its own cloud within the borders of South Africa in order to minimise security risk, like cross-border jurisdictions. According to De and Pal (2014), security is a technical factor that obviates the adoption of cloud storage. This clearly indicates that despite the advantages of cloud computing from a business perspective computing, there are still challenges like distrust of the cloud that one cannot control. It is daunting task to avoid risks; however, the essential issue is to identify and manage the risks the organisation is exposed to.

According to NARSA of 1996 and Erway (2010), electronic mails are born digital records. They need to be treated as the prescription of the NARSA. To have them privately hosted in the cloud while paper records are deemed to be prohibited by the Act is inconsistent. Any risk associated with digitalized paper records cannot be dissociated from born digital records that are stored in the cloud because they are regulated by one legislation. The current study demonstrates that government departments have started doing away with local exchange in favour of hosted exchange in order to have email services beyond workplace and business hours. These email services are hosted by the CSP through the SLAs entered into by the IT managers on behalf of the organisations. When the organisations grow, more allocation of space is purchased from the CSP in order to accommodate everyone in the organisation. This practice concurs with Sheng et al (2012) in which John McCarthy predicted that computation would be organised as a public utility. The prediction does not negate records management system in the cloud where the space can be purchased and allocated to the government in order to provide access to the public through e-government services.

6.2.3 Digital preservation of records in the cloud

Preservation forms part of the life cycle management of a records. Digital preservation ensures that records are stable and easily accessible for a longer period. Literature review indicates that digital preservation ensures that content in digital format remains accessible over time, reliable and authentic. Despite providing crucial records like finance, heritage and many more, it is capable of availing access to records that would have never been accessed. The public sector is able to preserve records on micro-film for its longevity. In this case, digital preservation of records takes place on the computer devices that are on the government premises. The results indicated that digital preservation is not taking place in the cloud, but on computer devices that are stored on the government premises. This is informed by the fact that the public sector stores records on the government premises. Having preserved records on the premises limits accessibility to the records. However, this can be attributed to the lack of preservation or digitalisation policy and the digital strategy. The current preservation might be taking place on the computer devices without policy and guidelines in place.

6.2.4 Disposal of records in the cloud

The life cycle of records is a progression through distinct steps from creation to disposal. Disposal of records is crucial in the life cycle of records management. Literature review indicates that disposal can be applied in the form of archiving or destruction. It is believed that disposal creates space for other records. According to Franks (2013), the primary purpose of records retention and disposal is to ensure that records are retained for as long as necessary and then disposed of when they no longer have value. Furthermore, literature review indicates that it is difficult to dispose of records in the cloud storage due to its multi-tenancy model which the CSP uses to save operational costs. Any attempt to dispose of records by means of wiping a disc carries risks of affecting records of another client or fellow cloud consumers. This is caused by the fact that the CSP provides resources and partitioned discs that are shared amongst clients.

On the other hand, the current study established that it is not necessary to dispose of records in the cloud due to its elasticity. When the allocated space is full, the client can purchase more space which ultimately discourages disposal. The current method that is used to dispose of digital records in a paper-based storage is performed through drilling the hard disc. More

importantly, disposal decisions need more than one records management practitioner to make decisions. In order to embark on a disposal process, this study revealed that a disposal directorate or digitalisation section must be established. Given the nature of how committees work, it further emerged from this study that the formation of a disposal directorate is very important due to its stability when juxtaposed with the committee. It is perceived that committees have challenges to quorate meetings, resulting in postponement of the meetings, while a directorate would have acted as planned. On the other hand, it is believed that the majority of the records are not digitised, they need to be digitised and this can become a function of disposal directorate.

6.3 Conclusions

This section provides the conclusions to the study based on the investigations. The conclusions of the investigation are organised according to the objectives of the study presented in section 6.3.1 to 6.3.4. In addition to that, a proposed model is presented and discussed.

6.3.1 Legislative frameworks and policies used for cloud storage

Developed countries in Europe, Asia and America have legislated the use of cloud storage in order to boost the provision of e-government services to the citizens. This study revealed that South Africa does not have cloud legislation. In the event that an organisation intends to obtain cloud services, various pieces of legislation are consulted in order to form cloud information. Records management is still governed by the NARSA Act, which is considered outdated because of its emphasis on paper-based storage on government premises.

Despite the fact that South Africa has adopted ISO standards for the records management environment, the current study established that the availability of ISOs does not prove useful, because they are not adhered to. This is influenced by the fact that records management officials have not been trained to identify valuable records. Even though digital records are stored in an unstructured manner on the computer devices that are safely kept on government premises, it emerged from this study that policies, guidelines and file plan on digital storage have not been developed. The current study further established that senior managers do not have a focus on the records management section despite admitting that it forms part of their directorate.

6.3.2 Entrusting public sector records in the cloud storage

The literature review indicated that although public servants informally and unconsciously place some records in the cloud, government departments in South Africa are sceptical to entrust their data to the CSP due to a number of reasons, such as lack of trust of cloud storage, cross-border jurisdiction, legal implications, data privacy and security risk related to MISS. Currently, the public sector stores records in various formats, for example, paper and audio, on the government premises. This study revealed that South Africa is less confident to migrate to the cloud storage, because it is conscious about who owns the cloud. This means government records cannot be stored in a privately owned cloud due to fear of security risk. It emerged that migration can take place to the government-owned cloud within the borders of South Africa.

6.3.3 Digital preservation of records on the cloud

According to Adu (2015), digital preservation gives an assurance to the right to information law that the government would accumulate and maintain information that is authentic, verifiable and reliable. It is comprised of the digital life cycle management processes, spans and archive operations that consist of acquisition, ingest, metadata creation, storage, preservation management and access (Delaney & De Jong 2015). The public sector is persistent in preserving its records on the micro-film for the fact that it is not easily damaged and that it lasts for over 400 years. The preservation of digital records is only taking place on computer devices that are kept on the government premises. It is believed that digital preservation on the cloud avails records that would not have been accessed.

6.3.4 Disposal of records in the cloud

Records retention and disposition ensure that records are retained only for as long as necessary and then disposed of when they no longer have value. However, this study revealed that disposing in the form of permanent destruction of records in the cloud is not necessary, because the cloud is elastic. The consumers can increase the allocated space through purchasing another storage space in order to accommodate more records. Furthermore, this study established that disposal of records in the cloud proves difficult because of the multi-tenancy model that is used by the CSP to save costs. Any attempt to dispose through wiping hard discs might negatively impact on unintended records of other cloud consumers. However, using a private-off premise

cloud computing model where the IT infrastructure is dedicated to specific customer organization does not pose risk to other cloud tenants. It is suggested that in order to perform disposal successfully, the current study reveals that a disposal section should be established within the organisation.

6.4 Recommendations

This section proposes recommendations to address issues identified during the study. The recommendations address each of the research objectives of the study as follows:

6.4.1 Legislative frameworks and policies used for cloud storage

- It is clear from the study that there is no legislation that makes provision for storage of records in the cloud. This is evidenced by the participants who indicated that they consult numerous pieces of legislations in order to form cloud information. This is an indication that cloud storage is not legislated within the government of South Africa. This leaves government officials mystified about the ways to approach cloud storage. To have an effective records management system, the government must provide support by effectively promulgating cloud legislation. This will result in the realisation of the government's vision to improve government services through e-government services that are protected by the law. Due to its transparency, cloud legislation will benefit the public sector to make well-informed decisions in the event it intends migrating to the cloud, irrespective of the cloud owner.
- The government must consider amending the NARSA Act of 1996, which governs records management within the areas of the public sector in order to include new ways of storing records off campus that are not limited to virtual premises. Currently, this Act mainly makes provision for paper records, audio and micro-film, which defeats the ubiquitous accessibility of information online.
- Given that the government has adopted ISO standards for records management, it must create awareness in the records practitioners so that they can comprehend and identify the value of records. This will ensure that the country is in line with the world's countries by practice, not by just having copies of ISO standards.

- The government departments must develop new policies, guidelines and file plan on cloud storage in line with an updated NARSA Act and the suggested cloud legislation. This will lead to an improved legislative framework that is in line with developed countries such as Australia, Canada and many more whose dealings with the citizens are provided online.
- In cognisance of the fact that the Records Management directorate keeps the footprints of the organisation, government must employ officials who have studied towards the careers of records or knowledge or information management degrees in order to minimise appointing managers who are not focused on records management functions. Such managers must recommend relevant courses that their subordinates should attend in order to remain relevant in the fast-paced technology within the records management environment.
- The government should consider revising the academic curriculum, particularly for the field of records management in order to include IT-related subjects. This is informed by the fact that records management is heading towards the IT space where hybrid records management practitioners possess IT and information sciences background.
- The Records Management section must work closely with the IT section in order to ensure that the selection of cloud storage is compatible with the government's IT infrastructures. It is necessary to form part of ICT department, because most of the time it will focus on records that are digitised and migrated to the cloud.
- Awareness' seminars on the value of registries in the public sector must be created and driven by NARSSA so that their functions are also given precedence.

6.4.2 Entrusting public sector records to the cloud storage

- The government must develop a government-owned cloud or adopt existing clouds of the private CSP. In view of the former option, the study reveals that the public sector is confident to utilise the storage where the government is involved. The government must consider developing a government-owned cloud. This means that the government can adopt an existing cloud which is controlled by the CSP. However, the government must develop regulations that must be followed when contracting a CSP. Such regulations must address cross-border jurisdictions, sovereignty of cloud and many other legal ways that protect records when the organisation faces legal challenges.

- It emerged from this study that there are more than one records management section in the government departments. Many sections that perform similar functions compromise the organisation, because they compete for superiority, draft contracting policies and eventually interpret the legislation differently and merge duplicated records management sections into one section headed by the records manager. This will benefit the government as it will have streamlined responsibilities, accountabilities, regulations and improved accountability.

6.4.3 Digital preservation of records on the cloud

- The literature review indicates that digital preservation ensures that the content in digital format remains accessible over time, reliable and authentic. Higgins (2008) and Delaney and De Jong (2015) add that digital preservation should apply to both born digital and formatted content. The public sector must develop digital preservation in the cloud with an intention to enhance long-lasting accessibility and availability of records that would never have been accessed. Digital preservation reduces the risk that records will become inaccessible over time.

6.4.4 Disposal of records in the cloud

- Primarily, disposal of records entails archiving or retention and permanent destruction. The DCC Lifecycle model views the life cycle of a record as a progression through distinct stages from creation to disposal. Regardless of the storage method or medium, negation of these stages renders lifecycle of records incomplete, because records are created in the initial stage and finally disposed of. In this case, to address archiving which is accessible to anyone in need records, it is important for the state to have its cloud that has enough storage. However, in the situation where records are disposed in the form of destruction, cloud consumers must consider the complexity of multitenancy model used by the cloud host. The cloud host, which in this case must be a state, should design a cloud in consideration of permanent destruction that does not negatively impact records of other public institutions.
- The government must consider establishing a digitalisation and disposal section within the directorate of Records Management. Given that the current record services is

prominently paper-based records, this section will be responsible for digitalization of paper records, in the process, it will decide which records are destined for disposal in the form of preservation or permanent destruction in order to inform the national archivist, This section will be at privilege to know the life cycle of records, which includes creation, digitalisation up to the disposal stage. It will decide on what should be disposed of.

6.5 Proposed framework

The fifth objective of this study was to propose a framework for digital curation of records in the cloud in South Africa. A plethora of researchers such as Babbie and Mouton (2011) and Neuman (2011) point out that another significance of a theoretical framework is its competence to devise the means to select and prioritise concepts to be invested. It has been revealed in this study that record management takes place and it is within the auspices of NARSSA, which reports to the DAC. Most noticeably, the records are prominently paper, audio and microfilm. All of these records are safely stored on government premises where they are protected by the NARSSA No.43 of 1996. It has also been identified that anyone in need of a particular record must visit NARSSA or any designated building in the provinces. This is caused by the fact that the records are not hosted in the cloud. Furthermore, the study established that records cannot be on the cloud storage due to the absence of a legislation that supports cloud storage. The absence of cloud legislation was the prominent finding of this study because it is hindering accessibility of the records through e-government. This study established that even though the public sector has digital records on the computer devices that are securely locked on the government premises, cloud storage has not yet been fully adopted. It is hoped that the proposed framework will promote easy access of government records as digital curation and e-government would be included in the process. It is worth noting that transformation is not easily accepted as people prefer to work comfortably in the way that they have been taught and that lead to resistance to change.

The framework depicted in Figure 6.1 is not a prescription of digital curation of records in the cloud in South Africa however, it will assist the public sector to consider the use of digital records in order to become more accessible to the citizens. It cannot be prescriptive because each organization can use the software relevant to match its culture. This framework will be crucial when the public sector relocates digital records in a regulatory manner from the current

paper-based storage on government premises to the cloud storage. This will be preceded by the promulgation of cloud legislation in order to ensure that the relocation of records to the cloud is done in a regulatory manner or within the prescripts of the law. The proposed framework achieves its purpose by paving the way that makes the use of cloud storage to enhance ubiquitous access of records by the general public. It presents the solution to the current situation in which records are confined to the government premises where the public gains access by visiting the physical archival holdings. As opposed to the current storage practice, which requires travelling expenses from the citizens that need access to the records, it induces interest in how citizens can access the records and information anywhere at any time. In this way, digital curation of records in the cloud in South Africa will transform accessibility of records to the general public. The proposed framework is flexible for expansion where other constituent parts can be introduced to the benefit of extended access of digital records.

It is not intended to impose relocation to the cloud, but to induce interest in how the citizens can benefit by accessing information ubiquitously in order to increase research productivity in this field. This proposed framework is based on Chapter Two, Chapter Four and Chapter Five of the current study. Some aspects discussed in Chapter Two indicate the benefits that other governments of other countries and financial sectors are enjoying the benefits of cloud. With the use of cloud, which has been coined government-cloud, the government is transparent to the citizens. In the financial sector, clients virtually interact with their financial institutions without physically visiting the branch. Chapter Four presented data from the participants wherein the key-role players (CIOs and records practitioners) indicated their lack trust in storing government records in the privately-owned cloud. In Chapter Five, the analysis on the collected data indicated that the participants have trust in government-owned cloud. Looking at that, the government cloud must be developed so that public institutions can utilise it to curate government records. It is proposing a framework that explains digital curation of records in the cloud in South Africa. It is also worth mentioning that there is no prescribed software that can used to achieve this, it is up to the department to choose anyone from vendors in consideration of compatibility to what the departments intend to achieve.

The proposed framework in Figure 6.1 is made up of the following elements: cloud legislation and policy framework, preservation, cloud storage, disposal and e-government. Central to this proposed framework is digital curation of records. The line outside with the figure shows how cloud legislation has influence to other elements and ultimately at the provision of e-

government services. The arrows inside have been used to show how they relate to one another. The reliability of the system is dependent on the IT infrastructure, for example LAN/WAN provided by the IT section and compliance with documents uploaded by the records management practitioners. The framework anticipates providing virtual access in line with the view of Ferreira et al (2017) who indicate that digital preservation ensures that the content in digital format remains accessible over time, reliable and authentic. This means as opposed to the current situation where there is a need to travel to the archival holdings, it is anticipated that those in need of records will access them anywhere at any time. In the event that records are not accessible, the IT section and the Records Management section will jointly work together to resolve the glitches.

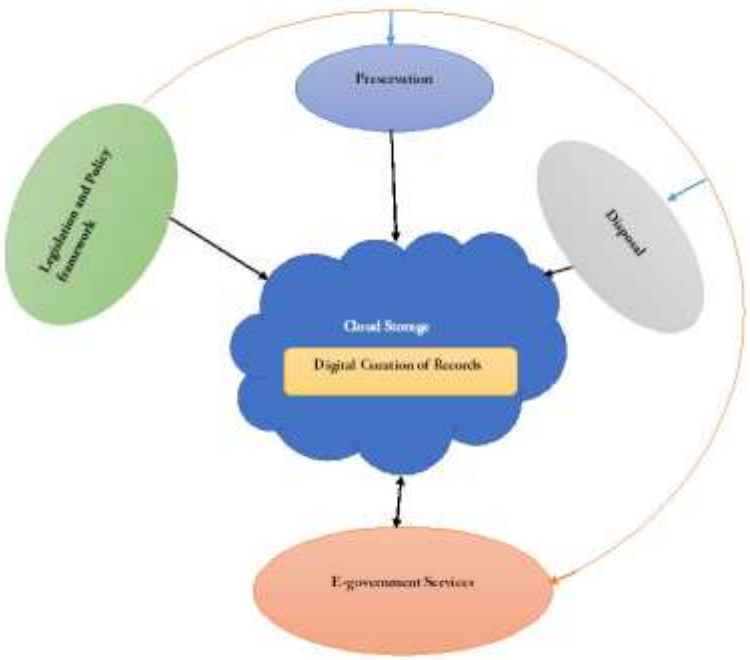

Figure 6.1 Framework for digital curation of records (Researcher 2019)

a) Legislation and policy framework

In South Africa, the responsibility of regulating government records falls under the auspices of NARSSA, which is a unit of the DAC. The NARSSA (No 43 of 1996) is the legislation that the government uses to regulate government records which are mainly paper-based. The legislation does not support cloud storage. Given the proliferation of ICT, records need to be accessed virtually by the citizens of the country in their convenient time. The study revealed that NARSSA (No 43 of 1996) was developed to regulate paper-based records of the government. Given the evolution of technology, the DAC should develop cloud legislation in order for the South African parliament to consider it before the president of the Republic enacts it. In consideration of the fact that this framework requires technology, the DAC should involve SITA from the premise that it has been given the responsibility to manage ICT in the government and its departments. As reflected in the framework, the implementation of this legislation should be driven to all government departments, nationally and provincially by the NARSSA. The cloud legislation should encourage all the government departments to migrate born digital and digitalised records to the cloud. This Act should be championed by NARSSA, where all government records are stored. The legislation should be accessible to all government departments and state institution. The Act must prescribe how the current records should be digitalised in preparation for digital curation in the cloud. As recommended, it should indicate who should be in charge with this process, for example, digitalisation section or digitalisation committee. This Act should indicate how records (born digital and digitalised records) and cloud storage are managed to the benefit the community through e-government services. This legislation will terminate confusion in the aspect of security and jurisdictions of records.

In order to have an effective digital curation, NARSSA must ensure that the government consider reviewing the current record-keeping policies in order to accommodate the cloud. This policy should be derived from cloud legislation in order to limit confusion during implementation. This policy can be drafted within the Registry section, in conjunction with the IT section. Given that South Africa subscribes to the ISO standards for archival holdings, the ISO standards on records keeping should always be adhered to as South Africa subscribes to the international standards of records keeping. These standards should be used closely with the cloud legislation. The government departments must develop cloud guidelines and file plan for cloud storage derived from cloud legislation and the reviewed NARSSA No. 43 of 1996. Act. These documents must be developed within the registry section by the records practitioners who have read the two pieces of legislation, for example, newly developed cloud legislation

and NARSSA. As depicted, every element on the framework relies on cloud legislation in order operate securely.

(b) Cloud storage

The government has born-digital and digitalised records stored on computer devices that are safely locked on government premises. This storing method supports digital curation of records only in a local environment. The use of these devices limits access the citizens to access information from anywhere at any time. Storing records opens the government to the citizens through e-government services. The government does not have a state-owned cloud storage. The current option that the government departments have for cloud storage is to use the CSP. However, the government's chances to control CSP on how to use its cloud are minimal. This creates lack of trust in using the CSP when considering that the service provider can be entangled in legal battle leading to the loss of records. the viability of cloud has been noticed when various government departments have their electronic mail services hosted by the CSP in order to communicate anywhere at any time, as the arrow shows, digital curation of records is not in a way that would have made accessibility to the citizens is reliant on the cloud. The government should develop a state-owned cloud storage where all government departments can purchase a storage space. In the government's cloud, digital curation will become simpler because all the departments might gain confidence to migrate records. The migration can commence with the already digitalised records stored on computer devices. However, the process should be guided by the digitalisation and disposal committee or section. This should be accompanied by legislative framework, cloud storage as well as SITA because it is responsible for ICT in the government. When it properly implemented, records that would not have been accessible are authentically made available.

(c) Preservation

Digital preservation of records takes place on the computer devices that are on the government premises. There is a need of digital curation records in a way that records are stable and accessible for a longer period. The use of physical storage on government premises does not promote ubiquitous access of preserved records anywhere at any time. The current way used by the government where those records are safely locked does not fulfil full access to everyone. The records need to be curated digitally and accessed in a cost-effective way. Digital preservation has minimal chances to damage records. Digital preservation should be enhanced

in the cloud with an intention to enhance long-lasting accessibility and availability of records that would never have been accessed.

(d) Disposal

Disposal is a crucial element in the lifecycle of records. Under normal circumstances, it is applied in the form of archiving/preservation or destruction with an intention to create space. When using digital curation of records in the cloud, the digitalisation and disposal section should review if disposal in the form destruction is still necessary because cloud space is elastic. However, in the event of disposal in the form of permanent destruction where formatting of discs is involve, it will have negative impact due to multi-tenancy model used by the CSP. Multi-tenancy model allows CSP to store records of various cloud clients on one portioned disc. When a record is digitalised, it is compressed into a smaller digital document that does not take more space. In this way, the record owners will have more space saved. The previous approach of disposing records should go through rigorous debate when there is a need to destroy.

(e) E-government

E-government is attainable through the through implementation of ICT infrastructure. ICT infrastructure creates a platform for cloud storage. Contribution of cloud storage to e-government services has the potential to merge distance and space, as well as reduce time, which makes the transactions of public service more effective. The safe delivery of e-government service is through the legislated platform where all government can participate without fear of losing information. All the records that are digitally curated can be accessed as determined by the digitalisation and disposal section. The vision of the South African government is to improve government services which, are regulated by cloud the cloud legislation. Furthermore, there will be a huge improvement in accessing information through e-government services if this framework were to be implemented. As opposed to the current situation where people still plan to visit the archival holdings, information will be a click away on their computer devices. As indicated in the diagram, e-government depicts the public accessing records or interaction between government and citizens. The bi-directional arrow between e-government and cloud storage indicates the interaction where information is queried from the e-government service to cloud storage. The other direction represents the response coming from cloud storage to the e-government service where the query was executed.

6.6 Implications for theory, policy and research

One other reason of pursuing research is to find solutions to identified research problems and provide recommendations. The recommendations are expected to close an identified gap. This entails that when the recommendations provided in this study are implemented, there might be a huge improvement in accessing information through e-government services. Leedy and Ormrod (2014) propound that research findings must be linked to what people already know, write about or believe in relation to the topic in question. The current study identified the challenges of migrating the paper-based records storage to the cloud. It is also believed that the current study will influence policy in the public sector, particularly the Department of Arts and Culture, which is the custodian of records management within the public sector. Should the recommendations of this study be recognised, the government will open itself to the public within the framework that is regulated by the government. Currently, the paper-based records management regulated by NARSA Act does not encourage people who are far away to access records due to the barrier it created by keeping records on government premises. This study is critical in doing away with the paper-based storage of records within the public sector and migrating to the cloud storage in case the proposed model of the current study is adopted. The earlier studies investigated the benefits of cloud computing and electronic services that the private sector has adopted to the betterment of the interaction with their clients. This study proposes the application of cloud storage in the public sector with a view to support e-government services in South Africa

6. 7 Further research

This empirical study breaks new ground that would require further in-depth research. As discussed in Chapter One and Chapter Three, there are indeed limitations and delimitations to this study that warrant further research.

- Given the generic approach to the establishment of a digitalisation and disposal section, extensive studies should be conducted in order to establish how best it can function to benefit the records management community.
- The evolution of technology takes place at a high speed. Further investigation should be made to establish how the curriculum can be reviewed in order to produce future

records management officials that will best fit in the new records management space without feeling marginalised.

- Given the elastic cloud that can store more records, it should be investigated whether there is still a need to go that route of disposing of records in the form of destruction since cloud storage space is becoming more available.
- Given the limited constructs used on the proposed model, it is suggested that other constructs be added in order to expand the study to the benefit of research communities and the country.
- The current study employed interviews for data collection, it is suggested that the future research use surveys or mixed methods for the future work.

6.8 Final conclusion

The current study consisted of six chapters where Chapter One outlined the study into perspective. Chapter Two reviewed literature covering legislative framework on record management and cloud computing. Chapter Three presented research methodology that was followed to conduct this study. This is where the methods were explained in details to ensure that the readers understood the target population and the type of data collected. In line with research methodologies, this gave a reasonable replication of this study. Chapter Four presented data of the study which came in the form of interviews and content analysis. Chapter Five presented the discussion of the findings which gave an idea of how to interpret the data. Chapter Six, the last chapter provided a summary of each chapter, summary of findings, recommendations in relation to the problem statement. In this chapter, a framework for digital curation of records was proposed in line with fifth objective.

Given the proliferation of ICT, the government should develop its state-owned cloud storage in order to allow all government departments to purchase the storage space. However, that should be preceded by developing a supportive legislation, particularly cloud storage. In the presence of cloud storage, digital curation of records can be enhanced where e-government can be easily achieved. It is worth noting that this study is appreciates the paper-based record management that NARSSA has performed over the years, now is time to leverage on the technology and take it digitally to the benefit of every citizen without limitation of distance and time. If this is not implemented, the record management will remain paper-based and the

citizens will remain closed out as far as accessibility of information through cloud service is concerned.

REFERENCES

Aas, K & Kärberg, T. 2010. Automated ingest of digital records from electronic records management Systems. Challenges e-2010 Conference Proceedings Paul Cunningham and Miriam Cunningham (Eds) *IIMC International Information Management Corporation, Maui*, HI, USA, 27-29 October.

Adu, KK. 2016. *Framework for digital preservation of electronic government in Ghana*. PhD Thesis. University of South Africa, Pretoria

Adu, KK, Dube, L & Adjei, E. 2016. Digital preservation: the conduit through which open data, electronic government and the right to information are implemented. *Library Hi Tech* 34(4): 733-747.

Alasuutari, P, Bickman, L & Brannen, J. 2008. *The sage handbook of social research methods*. London: Sage.

Alexander, S. 2014. Implementing right to information: a case study of the United States. In: Trapnell, S.E. (ed), *Right to information: Case on implementation.* Right to information series, World Bank: Washington DC, 539-624. Available at: http://siteresources.worlbank.org/ (Accessed 13 March 2019).

Almeida, MB, Cendón, BV & Souza, RR. 2012. Methodology for digital document preservation program implementation long term. *Meeting Bibli: Electronic Journal of Library and Information Science* 17(34): 103-130.

Al-Rashidi, H. 2013. *The role of internal stakeholders and influencing factors during the phases of e-government initiative implementation*. PhD Thesis, Brunel University, London.

AlZain, MA, Pardede, E, Soh, B & Thom, JA. 2012. Cloud computing security: from single to multi-clouds. *45th Hawaii International Conference on System Sciences,* 5490-5499. https://doi.org/10.1109/HICSS.2012.153.

Ambira, CM. 2016. *A framework for management of electronic records in support of e-government in Kenya*. PhD Thesis, University of South Africa, Pretoria.

An, X, Bai, W, Deng, H, Sun, S, Zhong, W & Dong, Y. 2017. A knowledge management framework for effective integration of national archives resources in China. *Journal of Documentation* 73(1)18-34. https://doi.org/10.1108/JD-04-2016-0040.

Anand, A, Ryoo, J & Kim, H. 2015. Addressing security challenges in cloud computing – a pattern-based approach. 1st *International Conference on Software Security and Assurance, ICSSA, Suwon, Gyeonggi*, Korea Republic, Republic, (6)13-18.

http:doi.org/10.1109/icssa.2015.013.

Anderson, R. 2015. *Thematic content analysis (TCA): descriptive presentation of qualitative data*. Available at: www.wellknowingconsulting.org/publications/pdfs/ThematicContentAnalysis.pdf (Accessed 1 August 2019).

Arshad, NI, Milton, SK, Bosua, R & Mehat, M. 2014. Enterprise content management technologies supporting unified businesses. *International conference on information technology and multimedia (ICIMU),* 184-188. Putrajaya, Malaysia, 18-20 November.

Asaeed, N & Saleh, M. 2015. Towards cloud computing services for higher educational institutions: concepts and literature review. Cloud computing. *International conference on cloud computing,* Riyadh, Saudi Arabia, 26-29 April.

Assefa, T. 2001. (ed.) Promoting good governance and wider civil society participation in Eastern and Southern Africa. *Report of Regional Conference, Addis Ababa, Ethiopia*, 6-8 November 2000.

Assyne, N & Riungu-Kalliosaari, L. 2014. A framework for implementing cloud computing for records sharing and accessing in the Ghanaian healthcare sector. *IST-Africa Conference proceedings,* Le Meridien Ile Maurice, Mauritius, 7-9 May.

Atkinson, E. 2002. Much ado about metadata. *Records Management Journal* 12(1): 19-23.

Babbie, ER & Mouton, J. 2011. *The practice of social research*. Cape Town: Oxford University Press.

Babbie, ER, Halley, F & Zaino, J. 2003. *Adventures in social research: data analysis using SPSS 11.0/11.5 for Windows.* 5th ed. California: Pinee Forge Press.

Babbie, ER. 2001. *The practice of social research*. 9th ed. London: Wadsworth.

Babbie, ER. 2010. *The practice of social research*. 12th ed. Belmont: Wadsworth Cengage.

Bahari, SF. 2010. Qualitative versus quantitative research strategies: contrasting epistemological and ontological assumptions. *Jurnal Teknologi* 52(1): 17-28.

Bailey, CA. 2007. *A guide to qualitative field research*. Thousand Oaks: Sage Publications.

Banerjee, A & Chaudhury, S. 2010. Statistics without tears: populations and samples. *Industrial Psychiatry Journal* 19(1): 60-65.

Barateiro, J, Draws, D, Neumann MA & Strodl, S. 2012. Digital preservation challenges on software life cycle. *16th European conference on software maintenance and reengineering (CSMR), Szeged*. http://doi.org/10.1109/csmr.2012.63.

Beagire, N. 2006. Digital curation for science, digital libraries and individuals. *International Journal of Digital Curation* 1(1): 1-7.

Beagrie, N & Jones, M. 2001. *Preservation management of digital materials: a handbook.* London: South Bank University.

Bekker, MJ. 2016. *Digital governance in support of infrastructure asset management*. PhD Thesis, University of Groningen, Groningen.

Bellamy, M. 2013. Adoption of cloud computing services by public sector organisations. *In Proceedings of the 2013 IEEE World Congress on Services* (SERVICES 2013), Santa Clara, California, 28 June – 3 July. https//:doi.org/10.1109/services.2013.50.

Benbasat, I, Goldstein, DK & Mead, M. 1987. The case research strategy in studies of information systems. *MIS Quarterly* 11(3): 369-386.

Bernard, HR. 2002. *Research methods in anthropology: qualitative and quantitative methods.* 3rd ed. California: Altamira Press.

Bettacchi, A, Re, B. & Polzonetti A. 2017. E-government and cloud: security implementation for services. *Proceedings of the 4th International conference on eDemocracy and e-Government,* Quito, Ecuado, 19-21 April. https://doi.org/10.1109/icedeg.2017.7962516.

Bhana, P. 2008. The contribution of proper records record-keeping towards auditing and risk mitigation: Auditor-General of South Africa's perspective. *Paper presented at the 3rd Annual General Meeting of the South African Records Management Forum*, Midrand (South Africa), 10-11 November. Available at: http://www.khunkhwane.co.za/uploads/The%20Contribution%20of%20Proper%20Records%20Keeping%20towards%20auditing%20and%20risk%20mitigation%20%20Auditor%20General%20Perspective.pdf (Accessed 20 April 2019)

Bhandari, A, Gupta, A & Das, D. 2016. A framework for data security and storage in cloud computing. *International conference on computational techniques in information and communication technology*, New Delhi, India, 11-13 March.

Bhattacherjee, A. 2012. *Social science research: principles, methods and practices*. Florida: Creative Common Attributions.

Bless, C, Higson-Smith, C & Sithole, SL. 2013. *Fundamentals of social research methods: an African perspective*. 5th ed. Claremont: Juta.

Botswana National Archives Records Service. 2009. Botswana national archives and records service mission statement. Available at: www.gov.bw/index.php?option¼co (Accessed 18 December 2017).

Bouaziz, F. 2008. Public administration presence on the web: a cultural explanation. *The Electronic Journal of e-Government* 6(1): 11-22.

Bradford, S & Cullen, F. 2012. *Research and research methods for youth practitioners.*

London: Routledge.

Braun, V & Clarke, V. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3(2): 77-101.

Brender, N & Markov, I. 2013. Risk perception and risk management in cloud computing: results from a case study of Swiss companies. *International Journal of Information Management* 33(5): 726-733.

Bryman, A & Bell, E. 2007. *Business research methods.* 2nd ed. New York: Oxford University Press.

Bryman, A & Bell, E. 2011. *Business research methods.* 3rd ed. New York: Oxford University Press.

Bryman, A. 2012. *Social research methods.* New York: Oxford University Press.

Bulow, AE & Ahmon, J. 2011. *Preparing collections for digitization*. London: Facet Publishing.

Bwalya, KJ & Healy, M. 2010. Harnessing e-government adoption in the SADC region: a conceptual underpinning: *Electronic Journal of e-government* 8(1): 23-32.

Cachin, C, Haas, R & Vukolic, M. 2010. Dependable storage in the inter-cloud. *Research Report RZ.* Available at: 5http://www.simplecloud.org/ (Accessed 13 March 2019).

Carter, L & Bélanger, F. 2005. The utilization of e-government services: citizen trust, innovation and acceptance factors. *Information Systems Journal* 15: 5-25.

Chipeta, J. 2018. A review of e-government development in Africa: a case of Zambia. *Journal of e-Government Studies and Best Practices*, Vol 2018 https://doi.org/10.5171/2018.973845.

Choak, C. 2012. Asking questions: interviews and evaluations. In: S. Bradford & F. Cullen. *Research and research methods for youth practitioners*, 90-112. London: Routledge.

Clarke, V & Braun, V. 2013. Thematic analysis. In: AC. Michalos (Ed.) *Encyclopaedia of quality of life research*. New York: Springer.

Colicchio, C, Giovanoli, C & Gatziu, GS. 2015. A cloud readiness assessment framework: for enterprise content management and social software (e-collaboration) in small and medium sized enterprises. *Paper read at 3rd International Conference on Enterprise System,* Basel, Switzerland, 14-15 October.

Collins, KMT, Onwuegbuzie, AJ & Sutton, IL. 2006. A model incorporating the rationale and purpose for conducting mixed methods research in special education and beyond. *Learning Disabilities: A Contemporary Journal* 4: 67-100.

Collis, J & Hussey, R. 2009. *Business research: a practical guide for undergraduate and postgraduate students.* 2nd ed. New York. Palgrave Macmillan

Considine, M. 1994. *Public policy: a critical approach*. South Melbourne: Macmillan Education.

Constantopoulos, P & Dallas, C. 2008. Aspects of a digital curation agenda for cultural agenda or cultural heritage. *IEEE International conference on distributed human-machine systems.1-6.* Athens, Greece.

Constantopoulos, P, Dallas, C, Androutsopoulos, I, Angelis, S, Deligiannakis, A, Gavrilis, D, Kotidis, Y & Papatheodorou, C. 2009. Digital curation centre and unit: an extended digital curation lifecycle. *The International Journal of Digital Curation* 1(4): 34-45.

Conway, M, Moore, R, Rajasekar, A & Jean-Yves, N. 2011. Demonstration of policy-guided data preservation using iRODS. *International symposium on policies for distributed systems and networks.* Pisa, Italy, 6-8 June.

Cook, T. 2001. Archival Science and postmodernism: new formulations of old concepts. *Archival Science* 1(1):3-24.

Cooper, H & Hedges, L. 1994. *The handbook of research synthesis*. New York: Russell Sage Foundation.

Cooper, RC & Schindler PS. 2008. *Business research methods*. New York: McGraw-Hill.

Creswell, J. 2002. *Educational research: planning, conducting, and evaluating quantitative and qualitative research.* Merrill Prentice Hall: Upper Saddle River.

Creswell, JW & Garrett, AL. 2008. The movement of mixed methods research and the role of educators. *South African Journal of Education* 28: 321-333.

Creswell, JW & Plano-Clark, VL. 2011. *Designing and conducting mixed method research.* 2nd ed. Thousand Oaks, CA: Sage.

Creswell, JW. 1998. *Qualitative inquiry and research design: Choosing among five traditions.* London: Sage.

Creswell, JW. 2006. *Understanding mixed method research*. California: SAGE Publications.

Creswell, JW. 2009. *Research design: Qualitative, quantitative and mixed methods approaches.* 3rd edition. Thousand Oaks CA: Sage.

Creswell, JW. 2013. *Qualitative inquiry and research design: choosing among five approaches.* Kindle ed. USA: SAGE Publications.

Creswell, JW. 2014a. *A concise introduction to mixed methods resea*rch. USA: Sage

Creswell, JW. 2014b. *Educational research: planning, conducting, and evaluating quantitative and qualitative research*. Enhanced Pearson e-text version-access card. 5th ed. Boston: Pearson.

Creswell, JW. 2014c. *Research design: qualitative, quantitative and mixed methods approach*. 4th ed. Los Angeles: Sage Publications Inc.

Cryer, P. 2006. *The research student's guide to success*. 3rd ed. Berkshire. Open University Press.

Cunningham, A. 2008. Digital curation/digital archiving: A view from the National Archives of Australia. *The American Archivist: Fall/Winter 2008* 71(2): 530-543.

Dahiru, AA, Bass, J & Allison, I. 2014. Cloud computing: Adoption issues for sub-Saharan Africa SMEs. *The Electronic Journal of Information Systems in Developing Countries* 62(1): 1-17.

Dale, JP. 2011. Introduction to cloud computing. *Journal of Electronic Resources in Medical Libraries* 8(4): 449-458.

Davies, JH. 1960. The organisational development of the Government Archives of the Union of South Africa. *South African Archives Journal* 2: 7-19.

De Lange, J, Von Solms, R & Gerber, M. 2016. Information security management in local government, in Cunningham, P, Cunningham, M. (eds). 2016. *IST-Africa Week Conference, Durban, South Africa*, 11-13 May. Available at: http://www.ist-africa.org/Conference2016 (Accessed 13 January 2018).

De Vos, AS, Strydom, H, Fouche, CB & Delport, CSL. 2011. *Research at grass roots: for the social sciences and human service professions.* 4th ed. Pretoria: Van Schaik.

De Vos, P. 2013. The newer, tamer Secrecy Bill: Still not constitutional. *Daily Maverick* 2013-05-07. Available at: http://www.dailymaverick.co.za/opinionista/2013-05-07-the-new-tamer-secrecy-bill-still-not-constitutional (Accessed 27 November 2017).

De, SJ & Pal, AK. 2017. A policy-based security framework for storage and computation on enterprise data in the cloud. *47th Hawaii international conference on system sciences*. Waikoloa, HI, USA, 6-9 January.

Dečman, M & Vintar, M. 2013. A possible solution for digital preservation of e- government: A centralised repository within a cloud computing framework. *Aslib Proceedings* 65(4): 406-424.

Delaney, B & De Jong, A. 2015. Media archives and digital preservation: overcoming cultural barriers. *New review of information networking* (20): 1-2.

Delaney, B & De Jong, A. 2015. Media archives and digital preservation: overcoming cultural

barriers. *New Review of Information Networking* 20: 73-89.

Doran, C. 2012. Governing the social network: How US Federal Department and Agency records management policies are addressing social media content. *Proceedings of the 45th Hawaii International Conference on System Sciences,* Maui, HI. USA https://doi.org/10.1109/hicss.2012.296

Duranti, L & Jansen, A. 2013. Records in the cloud: authenticity and jurisdiction. *Proceedings at the Digital Heritage International Congress (DigitalHeritage), 161-164.* https://doi.org/10.1109/digitalheritage.2013.6744748.

Ebaid, IE. 2011. Internal audit function: an exploratory study from Egyptian listed firms. *International Journal of Law and Management* 53(2): 108-128.

Ebrahim, Z & Irani, Z. 2005. E-government adoption: architecture and barriers. *Business Process Management Journal* 11(5): 589-611.

Electronic Communications and Transactions Act. 2002. Digital Society SouthAfrica: South Africa's National e-Strategy towards a thriving and inclusive digital future. Available at: www.gpwonline.co.za [Accessed 18 November 2019].

Erway, R. 2010. Born digital. OCLC research. *OCLC Online Computer Library Center, Inc*. Available at: http://oclc.org/research/activities/hiddencollections/borndigital.pdf (Accessed 18 April 2018).

Etikan, I, Musa, SA & Alkassim, RS. 2016. Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics* 5(1): 1-4.

Evans, C. 2018. *Analysing semi-structured interviews using thematic analysis: exploring voluntary civic participation among adults*. London: SAGE Publications.

Ferreira, MA, Drummond, AC & De Araujo, PF. 2017. Performance evaluation of a private cloud storage infrastructure service for document preservation. *12th Iberian conference of information systems and technologies,* Lisbon, Portugal, 21-24.

Franks, PC. 2013. *Records and information management.* Chicago: Neal-Schuman.

Franks, PC. 2015. Government use of cloud-based long-term digital preservation as s service: an exploratory study. *Digital Heritage,* Granada, Spain, 28 September -2 October.

Gangwar, H, Date, H & Ramaswamy, R. 2015. Developing and cloud computing adoption framework. *Global Business Review* 16: 632-651.

Garcia-Galan, J, Trinidad, P, Rana, OF & Ruiz-Cortes, A. 2016. Automated configuration support for infrastructure migration to the cloud. *Computer systems* 55 200-212.

Geerts, F, Kementsietsidis, A & Milano, D. 2006. Mondrian: Annotating and querying databases through colours and blocks. *Proceedings of the international conference on data engineering, Milano,* 3 May

Gerber, M, Solms, R & Overbeek, P. 2001. Formalizing information security requirements. *Information and Management Computer Security* 9(1).

Gerring, J. 2012. *Social science methodology: a unified framework.* 2nd ed. Cambridge: Cambridge University Press.

Gibson, J, Rondeau, R, Eveleigh, D & Tan, Q. 2012. Benefits and challenges of three cloud computing service. *Proceedings of the 2012 4th International Conference on Computational Aspects of Social Networks, Cason,* 1 November. https://doi.org/10.1109/cason.2012.6412402.

Glesne, C & Peshkin, A. 1992. *Becoming qualitative researchers: An introduction*. White Plains, New York: Longman.

Gomm, R. 2008. *Social research methodology: a critical introduction*. 2nd ed. New York: Palgrave MacMillan.

Gonzales, D, Kaplan, JM, Saltzman, E, Winkelman, Z & Woods, D. 2017. Cloud-trust - a security assessment model for infrastructure as a service (IaaS) Clouds. *Transactions on cloud computing* 5(3).

Gonzalez, N, Miers, C, Redígolo, F, Carvalho, T, Simplicio, M, Näslund, M & Pourzand, M. 2011. A quantitative analysis of current security concerns and solutions for cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications* 1(11).

Grobauer, B, Walloschek, T & Stocker, E. 2011. Understanding cloud computing vulnerabilities. *IEEE Security & Privacy Magazine* 9(2): 50-57.

Gubrium, JF & Holstein, JA. 2001. *Handbook of interview research: context and method.* Thousand Oaks: Sage.

Halbert, M, Skinner, K & McMillan, G. 2009. Avoiding the calf-path: Digital preservation readiness for growing collections and distributed preservation networks. In *Archiving Conference. Society for Imaging Science and Technology* (1): 86-91.

Hamdi. M. 2012. Security of cloud computing, storage, and networking. *Proceedings of the 2012 International Conference on Collaboration Technologies and Systems*, Denver, CO, USA, 21-25 May.

Han, Y. 2013. IaaS cloud computing services for libraries: cloud storage and virtual machines, OCLC Systems & Services: *International digital library perspectives* 29(2): 87-100.

Hare, CE & Mcleod, J. 1997. *Developing a records management programme.* London: Aslib.

Harwell, RM. 2011. Research design in qualitative/quantitative/mixed methods. In: *The Sage handbook for research in education pursuing ideas as the keystone of exemplary inquiry*. 2nd ed. Thousand Oaks: Sage, 147-163.

Hashemi, S, Monfaredi, K & Masdari, M. 2013. Using cloud computing for e-government: Challenges and benefits, *World Academy of Science, Engineering and Technology, International. Science Index 81, International Journal of Information Science and Engineering*, 7(9): 987-995.

Heidorn, PB. 2011. The emerging role of libraries in data curation and e-science. *Journal of Library Administration* 51(7-8): 662-672.

Heslop, H, Davis, S & Wilson, A. 2002. *An approach to the preservation of digital records*. Canberra: National Archives of Australia.

Higgins, S. 2008. The digital curation centre lifecycle model. *International Journal of Digital Curation* 3(1): 134-140.

Higgins, S. 2011. Digital curation center: The emergence of a new discipline. *The International Journal of Digital Curation* 2(6).

Hitchcock, G & Hughes, D. 1995. *Research and the teacher: a qualitative introduction to school-based research.* 2nd ed. London: Routledge.

Hsiung, P. 2012. The globalization of qualitative research: challenging Anglo-American domination and local hegemonic discourse. *Forum: qualitative social research* 13(1): 1-13. Available at: http://www.ualberta.ca/~iiqm/backissues/3_1/pdf/groenewald.pdf (Accessed 9 January 2018).
http://libguides.usc.edu/content.php?pid=83009&sid=618409 (Accessed 10 January 2018).

Hu, G, Wang, J, Pan, W & Shi, J. 2011. Impact antecedents of e-government content service capability: An exploratory empirical study. *Proceedings of 2011 international conference on business computing and global informatization*, Shangai, 29-31 July.

International Organisation for Standardisation (ISO). 2001. ISO 15489. *What-is electronic-records-management*? Available at: http://www.aiim.org/ (Accessed 8 March 2018).

International Records Management Trust. 1999. *A model records and archives law, International Records Management Trust.* Available at: http://www.irmt.org/documents/educ_training/.../IRMT_archive_law.doc (accessed on 25 March 2019).

Jackson, M & Shelly, M. 2012. *Electronic Information and the Law*. Sydney: Thomson Reuters Professional Australia Limited.

Jamsa, K. 2014. *Cloud computing 2013*. USA: Jones & Barlett Learning.

Jing, Z & Fang, Z. 2017. A study on library service innovation based on data curation. *Proceedings of the 13th International Conference on Semantics, Knowledge and Grids*, Bijing, China, 13-14 August

Johnson, RB & Christensen, I. 2008. *Educational research: qualitative and mixed approaches*. 3rd ed. Thousand Oaks: Sage Publications.

Johnson, RB & Onwuegbuzie, AJ. 2004. Mixed methods research: a research paradigm whose time has come. *Educational Researcher* 33(7):14-26.

Julisch, K & Hall, M. 2010. Security and control in the cloud. *Information Security Journal: A Global Perspective* 19: 299-309.

Kabata, V. 2012. *Outsourcing records storage to the cloud: challenges and prospects for African records managers and archivists*. Pretoria: UNISA Press.

Kaliannan, M, Awang, H & Raman, M. 2009. Government purchasing: a review of e-procurement system in Malaysia. *The Journal of Knowledge Economy and Knowledge Management IV Spring* IV: 27-41.

Kalusopa T. 2011. *Developing an e-records readiness framework for labour organisations in Botswana*. PHD Thesis, Pretoria, University of South Africa.

Kalusopa, T & Ngulube, P. 2012. Record management practices in labour organisations in Botswana. *South African Journal of Information Management* 14(1): 513.

Katuu, S & Ngoepe, M. 2015. Managing digital records in a South African public sector institution. *Conference: INFuture2015: e-Institutions – Openness, Accessibility, and Preservation*. At Zagreb. Croatia.

Keakopa, SM. 2010. *Management of electronic records*. Lap Lambert: Academic Publishing.

Kemoni, HN & Ngulube, P. 2007. National Archives and the effective management of public sector records in Kenya. *Mousaion* 25(2): 120-140.

Kim, S, Kim, HJ & Lee, H. 2009. An institutional analysis of an e-government system for anti-corruption: the case of OPEN. *Government Information Quarterly* 26: 42-50.

King, WR & He, J. 2005. Understanding the role and methods of meta-analysis in IS research. *Communications of the AIS* 16: 665-686.

Klein, HK & Myers, MD. 1999. A set of principles for conducting and evaluating interpretive field studies in information systems. *Evaluating interpretive field studies (23)* 67-94.

Komba, MM. & Ngulube, P. 2012. E-government adoption in developing countries: trends in the use of models. *ESARBICA Journal* 30(1): 162-176.

Kong, W & Lei, Y. 2016. Data security and privacy information challenges in cloud

computing. *International Conference on Intelligent Networking and Collaborative Systems.*

Kothari, CR. 2004. *Research methodology, methods and techniques.* 2nd ed. New Delhi: International Publishers.

Kriesberg, A, Huller, K, Punzalan, R & Parr, C, 2017. An analysis of federal policy on public access to scientific research data. *Data Science Journal* 16-27.

Kriesberg, A. 2017. The future of access to public records? Public-private partnership in United States and territorial archives. *Archival Science* 17:5.

Kriesberg, AM. 2015. *The changing landscape of digital access: public-private partnerships in US state and territorial archives*. Michigan: University of Michigan.

Kroukamp, H. 2005. E-governance in South Africa: are we coping? *Acta Academica* 37(2): 52-69.

Kuiper, E, Van Dam, F, Reiter, A & Janssen, M. 2014. *Factors influencing the adoption of and business case for cloud computing in the public sector*. Available at: www.echallenges.org. (Accessed on 18 June 2017).

Kulkarni, G, Gambhir, J, Patil, T, Dongare, A. 2012. A security aspect in cloud computing. *Proceedings of the International Conference on Computer Science and Automation Engineering*. http://doi.org/10.1109//icsess.2012.6269525.

Kumar, P, Sehgal, VK, Chauhan, DS, Gupta, PK & Diwakar, M. 2011. Effective ways of secure, private and trusted cloud computing. *International Journal of Computer Science Issues* 8(3): 412-421.

Kumar, R. 2005. *Research methodology: a step-by-step guide for beginners*. London: Sage.

Labaree, R.V. 2013. *Organising your Social Sciences Paper*. California: University of California.

Laudon, KC & Laudon, JP. 2015. *Management Information Systems: Managing the Digital Firm Plus MyMISLab with Pearson eText.* 14th ed. New Jersey: Prentice Hall Press.

Leedy, PD & Ormrod, JE. 2005. *Practical research: planning and design*. New Jersey: Pearson.

Leedy, PD. & Ormrod, JE. 2010. *Practical research: planning and design.* 9th ed. New Jersey: Pearson Education.

Leedy, PD. & Ormrod, JE. 2013. *Practical research: planning and design.* 10th ed. New Jersey: Pearson Education, Inc.

Leedy, PD. 1997. *Practical research: planning and design*. 6th ed. London: Prentice-Hall.

Liang, J. 2012. Government cloud: Enhancing efficiency of E-government and providing better public service. *International Joint Conference on Service Sciences Government* 261-265. https://doi.org/10.1109/ijcss.2012.20.

Liang, Y, Qi, G, Wei, K & Chen, J. 2017. Exploring the determinant and influence mechanism of e-Government cloud adoption in government agencies in China. *Government Information Quarterly* 34: 481-49.

Locke, LF, Silverman, SJ & Spirduso, WW. 2010. *Reading and understanding research.* 3rd ed. Thousand Oaks CA: Sage.

Low, C, Chen, Y & Wu, M. 2011. Understanding the determinants of cloud computing adoption. *Industrial Management & Data Systems* 111(7): 1006-1023.

Lu, Y & Ramamurthy, K. 2011. Understanding the link between information technology capability and organizational agility: *An empirical examination. MIS Quarterly* 35(4): 931-954.

Lwonga, ET, Ngulube, P & Stilwell. 2011. Challenges of managing indigenous knowledge with other knowledge with other knowledge systems for agricultural growth in sub-Saharan. *Library Review* 61(3): 226-238.

Lysaght, Z. 2011. Epistemological and paradigmatica ecumenism in Pateur's Quadrant: Tales from doctoral research. Ocial Conference Proceedings of the third Asian conference on Education in Osaka, Japan. Available at http://iafor.org/ace2011 _o print_0254.pdf (Accessed on 20 November 2017).

Mail & Gurdian. 2019. SA artists' call to Ramaphosa: Stop making Arts & Culture a dumping ground for delinquent Ministers Daily Maverick. Available at: https://mg.co.za › 2019-06-04-00-arts-sidelined-in-ramaphosas-new-cabinet (Accessed 010 June 2019).

Mackenzie, N & Knipe, S. 2006. Research dilemmas: paradigms, methods and methodology. *Issues in Educational Research* 16(2): 193-205.

Maluleka, JR. 2017. *Acquisition, transfer and preservation of indigenous knowledge by traditional healers in the Limpopo province of South Africa.* PhD Thesis, University of South Africa, Pretoria.

Marutha, MS. 2011. A framework to embed medical records management into the healthcare service delivery in Limpopo province of South Africa. PhD Thesis, University of South Africa, Pretoria.

Maxwell, JA. 2005. *Qualitative research design: An interactive approach.* 2nd ed. Thousand Oaks, CA: Sage Publications.

McMillan, JH & Schumacher, S. 2006. *Research in education Evidence-based inquiry* 6th ed. Boston, MA Allyn and Bacon.

McNeill, P & Chapman, S. 2005**.** *Research methods*. 3rd ed. London: Routledge.

Miles, MB & Huberman, AM. 1994. *Qualitative data analysis: An expanded source book.* 2nd ed. Thousand Oaks: Sage.

Miles, MB, Huberman, AM & Saldana, J. 2016. *Qualitative data analysis. A methods source book*. 3rd ed. Los Angeles: SAGE.

Mirashe, SP & Kalyankar, NV. 2010. Cloud computing. *Communications of the ACM* 51(7): 9.

Mittal, RL. 1971. *Public library law: an international survey*. New Delhi: Metropolitan Book Company.

Mizrahi, Y & Marcos, M. 2014. Implementing right to information: a case study of Mexico, right to information: case studies on implementation. *In: Trapnell, S.E. (ed.) Right to Information Series, World Bank, Washington*, 103-150.

Mnjama, N. & Wamukoya, J. 2006. E-government and records management: an assessment tool for records readiness in government. *The Electronic Library* 25(3): 274-284.

Mnjama, NM. 1996. National Archives and the Challenges of Managing the Entire Life Cycle of Records. *South African Archives Journal* 38: 24-32.

Mogale, TM. 2007. Local governance and poverty reduction in South Africa II: the role of micro-finance. *Progress in Development Studies* 7(4): 345-355.

Moghaddam, FF, Ahmadi, M, Sarvari, S, Eslami, M & Golkar, A. 2015. Cloud computing challenges and opportunities: a survey. *Proceedings of the 1st International conference on telematics and future generation networks*, 34-38: https://doi.org/10.1109/tagen.2015.7289571.

Mohammed, F, Ibrahim, O & Ithnin, N. 2016. Factors influencing cloud-computing adoption for e-government implementation in developing countries: instrument development. *Journal of Systems and Information Technology* 18(3): 297-327.

Monette, DR, Sullivan, TJ & Dejong, CR. 2011. *Applied social research: a tool for the human services*. New York: Brooks/Cole Cengage Learning.

Mouton, J. 2009. *Understanding social research*. 6th ed. Pretoria, Van Schaik Publishers.

Mutkoski, S. 2015. National Cloud Computing Legislation Principles: Guidance for Public Sector Authorities Moving to the Cloud. *IEEE International Conference on Cloud Engineering (IC2E).* https://doi.org/10.1109/ic2e.2015.104.

Mvelase, P, Dlamini, Z, Macleod, D, Dlodlo, N & Sithole, H. 2013. A business model for a

South African government public cloud platform. *IIMC International Information Management Corporation.*

Mwangi, FG. 2012. The road to providing access to Kenya's information heritage: digitization project in KNADS. *Proceedings of an international conference on permanent access to digital documentary heritage. Vancouver*, September: 82-91. Available at: http//:www.ciscra.org (Accessed 26 July 2014).

Myers, MD. & Newman, M. 2007. The qualitative interview in IS research: *Examining the craft. Information and Organisation* 17(1): 2-26.

Myers, MD. 2013. *Qualitative research in business and management*. London: Sage.

Nam. T. 2012. Citizens' attitudes toward open government and government 2.0. *International Review of Administrative Sciences* 78*:* 346-368.

National Archives and Records Administration. 2010. Open government plan, National Archives and Records Administration, College Park.

National Archives and Records Service of South Africa. 2006. *Records Management Policy Manual.* NARS, Pretoria.

National Archives and Records Service of South Africa. 2007. *Records management policy manual.* Pretoria: NARS. Available at: http://www.national.archives.gov.za/rms/Records_Management_Policy_Manual_October_2007.pdf (Accessed 12 January 2018).

National Archives of U.K. 2014. The Technical Registry PRONOM. Available at: http://www.nationalarchives.gov.uk/PRONOM/ (Accessed 18 December 2017).

Ndenje-Sichalwe, E. 2010. *The significance of records management to fostering accountability in the public service reform programme of Tanzania*. PhD Thesis, University of KwaZulu-Natal, Pietermaritzburg.

Neuman, WL. 1991. *Social research methods: qualitative and quantitative approaches.* Boston: Allyn and Bacon.

Neuman, WL. 1997. *Social research methods. Qualitative and quantitative approaches*. Boston, London Toronto: Allyn & Bacon.

Neuman, WL. 2006. *Social research methods: Qualitative approaches*. 6th ed. Boston: Allyn and Bacon.

Neuman, WL. 2011. *Social research methods: qualitative and quantitative approaches.* 7th ed. Boston: Allyn and Bacon

Neuman, WL. 2013. *Social research methods: qualitative and quantitative approaches.* Boston: Allyn and Bacon

Neville, C. 2010. *The complete guide to referencing and avoiding plagiarism*. 2nd ed. Bergshire: Open University Press.

Ngoepe M. & Nkwe, M. 2018. Separating the wheat from the chaff with the winnowing fork. *Records Management Journal* 28(2): 130-142.

Ngoepe, M & Saurombe, A. 2016. Provisions for managing and preserving records created in networked environments in the archival legislative frameworks of selected member states of the Southern African Development Community. *Archives and Manuscripts* 44(1): 24-41.

Ngoepe, M & Van der Walt, T. 2010. A framework for a records management programme: lessons from the department of cooperative governance and traditional affairs in South Africa. *Mousaion* 28(2): 82-106.

Ngoepe, M. 2011. *Records management process in the South African public sector: Challenges, trends and issues.* Saarbrücken: Lambert Academic Publishing.

Ngoepe, M. 2012. *Fostering a framework to embed the records management function into the auditing process in the South African public sector*. PhD Thesis, University of South Africa, Pretoria.

Ngoepe, M. 2014. The role of records management as a tool to identify risks in the public sector in South Africa, *SA Journal of Information Management* 16(1)8.

Ngoepe, M. 2017. Archival orthodoxy of post-custodial realities for digital records in South Africa. *Archives and Manuscript.*

Ngoepe, MS. 2008. *An exploration of records management trends in the South African public sector: A case study of the department of provincial and local government.* MINF Dissertation, University of South Africa, Pretoria.

Ngulube P, Mathipa, ER & Gumbo, MT. 2015. Theoretical and conceptual framework in the social sciences. In: ER. Mathipa & MT. Gumbo (eds.) *Addressing Research Challenges: Making headway in developing researchers.* Mosala-Masedi Publishers & Booksellers cc: Noordywk, 43-66.

Ngulube, P. 2012. Ghost in our machines: preserving public digital information for the sustenance of electronic government in sub-Sahara Africa. *Mousaion* 30(2): 128-136.

Nguyen, QL & Lake, A. 2011. Content server system architecture for providing differentiated levels of service in a digital preservation cloud. *Proceedings of the 4th International Conference on Cloud Computing*, Washington, DC, USA, 4-9 July Available at: http://10.1109/cloud.2911.73 (Accessed 20 May 2019).

Ning, W., Xiaoshan, X., Li hui, Xuehua, W. & Xuezhi Q. 2015. Survey of application and

research on government cloud computing in China. *Proceedings of the International Conference on Web Intelligence and Intelligent Agent Technology*: https://10.1109/wi-iat.2015.194. Singapore, Singapore 6-9 December.

Nyide, BC. 2014. *The digitisation of theses and dissertations at the University of Kwa-Zulu-Natal*. Durban. PhD Thesis, University of Kwa-Zulu Natal, Pietermaritzburg.

Ojo, JS. 2014. E-governance: an imperative for sustainable grass root development in Nigeria. *Journal of Public Administration and Policy Research* 6(4): 77-89.

Oredo, J, Njihia, J & Iraki, XN. 2017. The role of organizing vision in cloud computing adoption by organizations in Kenya. *American journal of information systems* 5(1): 38-50.

Oyewole, OA. 2012. The evolution of records management in sub-Saharan Africa. *Information and Records Management Bulletin* 166(March): 3-4.

Pan, W. 2019. *Managing records as evidence and information in china in the context of cloud-based services*. PhD Thesis. The University of British Columbia, Vancouver.

Pappel, I, Pappel, I & Saarmann, M. 2012. Digital records keeping to information governance in Estonian local governments. *International Conference on Information Society*.

Paquette, S, Jaeger, PT & Wilson, SC. 2010. Identifying the security risks associated with governmental use of cloud computing. *Government Information Quarterly* 27: 245-253.

Park, SC & Ryoo, SY. 2012. *An empirical investigation of end-users switching toward computing: A two-factor theory perspective*. Elsevier Ltd.

Patton, MQ. 1990. *Qualitative evaluation and research methods*. 2nd ed. Newbury Park, CA: Sage.

Patton, MQ. 2002. *Qualitative research and evaluation methods*. 3rd ed. Thousand Oaks, CA: Sage.

Patton, MQ. 2005. *Qualitative Research.* Wiley Online Library.

Pederit, R. & Mainoti, G. 2016. Mitigating user concerns to maximize trust on cloud platforms. *1st-Africa week conference.* https://doi:10.1109/1stafrica.2016.7530691IIMC.

Peekhaus, W. 2011. Biowatch South Africa and the Challenges in enforcing its constitutional rights to access to information. *Government Information Quarterly* 28: 542-552.

Pickover, P & Harris, V. 2001. Freedom of information in South Africa: a far off reality? Johannesburg: South African History Archive. Available at: http://www.wits.ac.za/saha/publications/FOIP_1_4_PickoverHarris.pdf (Accessed 14 April 2019).

Plano-Clark, VL. 2010. The adoption and practice of mixed methods: US trends in federally

funded health-related research. *Quantitative Inquiry* 16(6)428-440.

Polyviou, A. & Pouloudi, N. 2015. Understanding adoption decision in the public sector. *Proceedings of the 48th Hawaii international conference on system sciences*. IEEE computer society. Kauai, HI, USA 5-8 January.

Post, C, Chassanoff, A, Lee, CA, Rabkin, A, Zhang, Y, Skinner, K & Meister, S. 2019. Digital curation at work. *Modelling workflows for digital archival materials.* Proceedings of the ACM/IEE Joint conference on digital libraries. Champaign, IL, USA, 2-6 June https://doi.org/10.1109/jcdl.2019.00016.

Promotion of Access to Information Act 2000. Available at: www.gpwonline.co.za [Accessed 18 November 2019].

Ramgovind, S, Eloff, M & Smith, E. 2010. *The management of security in cloud computing. Information Security for South Africa*. Sandton, South Africa.

Randolph, J. 2009. A guide to writing the dissertation review. *Practical Assessment, Research and Evaluations* 14(13).

Reif, LC. 2004. *The ombudsman, good governance and the international human rights system*. Leiden: Martinus Nijhoff Publishers.

Republic of South Africa. (1996). *National Archives and Records of South Africa Act, No 43 of 1996*. Government Printers, Pretoria.

Republic of South Africa. 1996. Constitution of the Republic of South Africa, Chapter 2: Bill of Rights. Government Printers, Pretoria.

Reza Bazi, H, Hassanzadeh, A & Moeini, A. 2017. A comprehensive framework for cloud computing migration using Meta-synthesis approach. *The Journal of Systems and Software* (128): 87-105.

Rocha, F & Correia, M. 2011. Lucy in the sky without diamonds: stealing confidential data in the cloud, *Proceedings of the 1st international workshop of dependability of clouds, data centres and virtual computing environments*, Hong Kong, China, 27-30 June.

C. Rogers, C. 2015. Authenticity of digital records in practice. *Digital Heritage*, Granada, 395-398. https://doi: 10.1109/DigitalHeritage.2015.7419532.

Roper, M & Millar, L. (ed.). 1999. *Managing public sector records: a training programme. an introduction to the management of public sector records study programme*. London: International Records Management Trust.

Rubin, A & Babbie, E. 2010. *Essential research methods for social work.* New York: Brooks/Cole Cengage Learning.

Rubin, HJ & Rubin, IS. 2012. *Qualitative interviewing: The art of hearing data.* 3rd ed. Thousand Oaks: Sage.

Rusbridge, C., Burnhill, P., Ross, S., Buneman, P., Giaretta, D., Lyon, L & Atkinson. 2005. The Digital Curation Centre: A Vision for Digital Curation. *IEEE international symposium on mass storage systems and technology*, *Sardinia, (Italy),* 20-24 June https://doi.org/10.1109/JCDL.2019.00016.

Rutrell, Y. 2010. City of Miami takes citizen services to the cloud [E B/OL]. Available at: http://gcn.com/articles/2010/03/10/city-of-miami-microsoft-azure.aspx (Accessed 13 February 2018).

Ryan. MD. 2013. Cloud computing security: the scientific challenge, and a survey of solutions. *The Journal of Systems and Software* 86(9): 2263-2268.

Safa, NS, Sookhak, M, Von Solms, R, Furnell, SN, Ghani, A & Herawan, T. 2015. Information security conscious care behaviour formation in organisations. *Computer Security* 53: 65-78.

Saldana, J. 2013. *The coding manual for qualitative researchers*. 2nd ed. Los Angeles: SAGE Publications.

Sarantakos, S. 1993. *Social research*. Victoria, Australia: Macmillan Education.

Sarantakos, S. 2013. *Social research.* 4th ed. Palgrave Macmillan.

Sarkar, M & Kumar, S. 2016. A framework to ensure data storage security in cloud computing. *IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference*. New York, United States of America.

Saunders, M, Lewis, P & Thornhill, A. 2009. *Research methods for business students*, 5th ed. Harlow: Pearson Education.

Saunders, M, Lewis, P & Thornhill, A. 2012. *Research methods for business students.* 6th ed. Pearson Education.

Saunders, MS, Lewis, P & Thornhill, A. 2003. *Research methods for business students.* 3rd ed. London: Pearson Education Limited.

Schellnack-Kelly, I. 2013. *The role of records management in governance-based evidence, service delivery and development in South African communities*. PhD Thesis, University of South Africa, Pretoria.

Schwandt, TA. 2007. *The Sage Dictionary of Qualitative Inquiry*. 3rd ed. Thousand Oaks: SAGE Publication.

Shadbolt, N, O'Hara, K, Berners-Lee, T, Gibbins, N, Glaser, H, Hall, W & Schraefel, MC. 2012. Linked open government data: lessons from Data.gov.uk. *IEEE Intelligent Systems* 27(3): 16-24.

Sharma, T & Banga, VK. 2013. Efficient and enhanced algorithm in cloud computing. *International Journal of Software Computer Engineering* 13: 2231-2307.

Sheng, Y, Yang, J & Keskin, T. 2012. The evolution of IT towards cloud computing in China and US. *International Conference on Computational Problem-Solving, Leshan, (China),* 19-21 October. https://doi.org/10.1109/ICCPS.2012.63843321.

Shim, DC & Eom, TE. 2009. Anticorruption effects of ICT and social capital. *International Review of Administrative Sciences* 75: 99-116.

Shuijing, H. 2014. Data security: the challenges of cloud computing. *Sixth international conference on measuring technology and mechatronics automation*. Shanghai, China, 10-11 January.

Sierman, B. 2012. *OAIS.* Available at: http://digitalpreservation.nl/seeds/oais-2012-update/ (Accessed 20 January 2018)

Singleton, RA. & Straits, BC. 2010. *Approaches to social research*. 5th ed. New York: Oxford University Press.

Sprott, AA. 2012. Let me in the cloud analysis of the benefit and risk assessment of cloud platform. *Journal of Financial Crime* 20(1): 6-24.

Stacks, DW & Hocking, JE. 1992. *Essentials of communication research.* New York: HarperCollins.

Stančić, H, Rajh, A & Jamic, M. 2017. Impact of ICT on archival practice from the 2000s onwards and the necessary changes of archival science curricula: *MIPRO. IEEE*.

Stevens, M. 2013. *Ethical issues in qualitative research*. London: King's College.

Stuart, K & Bromage, D. 2010. Current state of play: records management and the cloud. *Records management journal. (20):217-225.*

Tao, F, Cheng, Y, Da Xu, L, Zhang, L & Hu Li, B. 2014. CClo T-CMfg: Cloud computing and internet of things-based cloud manufacturing service system. *IEEE Transactions on industrial informatics* (10)2.

Thomas, DR. 2003. *A general inductive approach for qualitative data analysis*. School of Population Health University of Auckland, New Zealand.

Thurston, A. 1996. Records management in Africa: old problems, dynamic new solutions. *Records Management Journal* 6(3): 187-199.

Trope, J. 2014. Adoption of cloud computing by South African firms: an institutional theory and Diffusion of Innovation theory perspective MINF Dissertation, University of Witwatersrand, Johannesburg.

Tsan-sheng, H, Hsin-Wen, W, Yen-Ping, H, Tseng-Yi, C, Tsung-Tai, Y, Mei-Ju, S, Yu-Chun, C & Wei-Kuan, S. 2014. A digital archive data preservation management system using iRODS architecture. *International Conference on Computational Science and Computational Intelligence.* IEEE.

Tzitzikas, Y, Kargakis, Y & Marketakis, Y. 2014. Assisting digital interoperability and preservation through advanced dependency reasoning. *International Journal on Digital Libraries* 15:103-127.

UNDESA. 2016. UN E-government survey 2016. *E-Government in Support of Sustainable Development*. Available at: doi.org/10.1016/S1369-7021(02)00629-6 (Accessed 12 August 2018).

UNISA. 2010. *Guidelines for master's and doctoral studies in Information Science*. Pretoria. Unisa.

UNISA. 2012. Policy on research ethics. Available at: http://www.unisa.ac.za/contents/research/docs/ResearchEthicsPolicy_apprvCounc_21Sept07.pdf (Accessed 15 January 2019).

United Nations e-government survey 2012. E-government for the people. *Economic and Social Affairs.* Available at: www.unpan.org/e-government (Accessed 15 February 2018)

Van der Schyff, K & Krauss, KEM. 2014. Higher education cloud computing in South Africa: Towards understanding trust and adoption issues. *South African Computer Journal* 55.

Van Jaarsveldt, LC & Wessels, JS. 2015. Information technology competence in undergraduate public administration curricula at South African universities. *International Review of Administrative Sciences* 1-18.

Venkatesh, V, Chan, FK & Thong, JY. 2012. Designing e-government services: Key service attributes and citizens' preference structures. *Journal of Operations Management* 30: 116-133.

Viana, P & Sato, L. 2014. A proposal for a reference architecture for long-term archiving, preservation, and retrieval of big data. In trust, security and privacy in computing and communications (TrustCom), *Proceedings of the IEEE 13th International Conference, Beijing, China,* 24-26 September.

Wahsh, MA & Dhillon, JS. 2015. An investigation of factors affecting the adoption of cloud computing for e-government implementation: An empirical study in Iraq. *IEEE Student*

Conference on Research and Development, 323-328.

Wai-Ming, T, Lai, LSL & Chung, AWL. 2013. Cloud computing in China: barriers and potential. *IT Professionals*, 15(3)48-53.

Wang, J & Zeng, T. 2009. Citizen-centered e-government strategy governance framework: Case of China, *International conference on Web information systems and mining. Shanghai*, 7-8 November.

Wanjiku, R. 2009. *Kenya Communication Amendment Act (2009): progressive or retrogressive.* Association for Progressive Communication. Available at: http:// www.apc.org (Accessed 1 February 2018).

Wimmer, M. 2004. Knowledge management in electronic government. *Proceedings of the 5th IFIP International Working Conference, KMGov 2004, Krems, Austria*, 17-19 May.

Xue, S. 2017. Reconstruction of records storage model on the cloud datacentre. *IEEE 11th International Conference on Semantic computing.* San Diego, CA, USA, 30 Jan.-1 Feb. 2017.

Yakel, E. 2006. Inviting the user into the virtual archives. OCLC Systems and Services: *International Digital Library Perspectives* 22(3): 159-163.

Yakel, E. 2007. Digital curation, OCLC Systems & Services: *International digital library perspectives* 23(4): 335-340.

Yang, Z, Zhang, L, Ding, W & Zheng, W. 2016. Heterogeneous data storage management with deduplication in cloud computing. *IEEE transactions on big data, manuscript id*. 1-14.

Yang, SQ. 2012. Move into the Cloud, shall we? *Library Hi-Tech News* 29(1): 4-7.

Yin, RK. 2017. *Application of case study research*. London: SAGE.

Yu, F. 2010. Case study of digital preservation for e-heritage: Digital preservation project for the collection of Penhas family. Proceedings of the *Conference on Management of e-Commerce and e-Government (ICMeCG)*. Chengdu, China, 23-24 October.

Yue, C, Xinhua B & Lei W. 2013. A study on user adoption of cloud storage service in China: a revised unified theory of acceptance and use of technology model. *International conference on information science and cloud computing companion.* Guangzhou, China, 7-8 December.

Yusuf, ZM & Chell, RW. 2005. *Issues in records management*. Bangi: Penerbit

Zhang, N, Yin, C, Meng, Q & Guo, X. 2014. The orientation-maturity framework for understanding the e-government key issues in China. *27th Hawaii International conference on system sciences*. Waikoloa, HI, USA, 6-9 January.

APPENDICES

APPENDIX A: INTERVIEW GUIDE

The purpose of this study was to explore entrusting records to the cloud to support e-government services in South Africa.

SECTION A: Demography

1. What position do you hold in this organisation?

Chief Information Officer	
IT Manager	
Records Manager	
Other, specify	

2. Who is responsible for management of digital records in your organisation?

SECTION B: Analyse policies and legislative frameworks used for records storage in the cloud in order to support e-government services

3. What are the standards and best practice indicators that have been adopted to guide the management of digital records in your organisation?

4. What legislations are used to govern cloud storage in your organisation?

5. What guidelines does your organisation follow to support cloud storage?

6. What policies do you use to support digital storage?

7. What e-government services are provided by your organisation?

8. What is the role of digital records in e-government?

9. What recommendations would you propose to improve the best practices and standards of managing cloud records in support of e-government?

SECTION C: Determine if public sector entrusts records in the cloud storage

10. Where do you store digital records?

11. Does your organisation entrust records in the cloud? If no, Why?

12. If yes, what cloud models are you using?

13. What are the terms and conditions for storage of records in the cloud?

14. How do you deal with security of records in the cloud?

15. Who have access to those records?

SECTION D: Analyse the public sector's view on digital preservation of records

16. How do you ensure that the records created are preserved for the future?

17. What are the benefits of digital preservation have you identified?

18. Is it necessary to have a management requirement concerning authenticity and security of digitally preserved records? Why?

19. What recommendations would you suggest to improve digital preservation of records?

SECTION E: Determine the processes followed to dispose records in the cloud.

20. How does this organisation dispose its digital records?

21. How do you determine that digital records are ready for disposal?

22. How do you get involved in the disposal process of digital records?

23. Do you think the formation of a disposal committee would add value in the disposal of digital records? Why?

SECTION F: Propose a framework that guides storage of records in the cloud in South Africa

24. Plenty of digital storages use for example, open archival information system (OAIS) model. Are you familiar with other models that can be applied in the digital environment? Give an example.

25. Would you prefer to use an existing model or a model specifically designed for your digital storage? Please give a reason.

26. Digital storage is reliant on IT; what prior knowledge do you suggest digital records officials should possess in order to use or understand the services of storage models?

27. What is the professional capacity that is required to support management of digital records?

Thank you for your participation in this project.

APPENDIX B: ETHICS CLEARANCE

UNISA university of south africa

DEPARTMENT OF INFORMATION SCIENCE ETHICS REVIEW COMMITTEE

22 November 2018

Dear Amos Shibambu

DIS Registration #: Rec-221118

References #: 2018-DIS-0006

Name: A Shibambu

Student #: 60873329

Decision:

Ethics Approval from 22 November 2018 to 20 November 2023

Researcher(s): Amos Shibambu

Supervisor(s): Prof Mpho Ngoepe

Application of cloud storage to support e-government services in South Africa.

Qualifications: PhD

Open Rubric

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

Thank you for the application for research ethics clearance by the Unisa Department of Information Science Research Ethics Committee for the above-mentioned research. Ethics approval is granted for five years.

The ***low risk application*** was reviewed and expedited by the Department of Information Science Research Ethics Committee on 22 November 2018 in compliance with the Unisa Policy on Research Ethics and the Standards Operating Procedure on Research Ethics Risk Assessment. The proposed research may now commence with the provisions that:

1. The researcher(s) will ensure that the research project adheres to the values and principles expressed in the UNISA Policy of Research Ethics.
2. Any adverse circumstances arising in the undertaking of the research project that is relevant to the ethicality of the study should be communicated in writing to the Department of Information Science Ethics Review Committee.
3. The researcher(s) will conduct the study according to the methods and procedures set out in the approved application.
4. Any changes that can affect the study-related risks for the research participants, particularly in terms of assurances made with regards the protection of participants' privacy and the confidentiality of the data should be reported to the Committee in writing, accompanied by a progress report.
5. The researcher will ensure that the research project adheres to any applicable national legislation, professional codes of conduct, institutional guidelines and scientific standards relevant to the field of study. Adherence to the following South African legislation is important, if applicable: Protection of Personal Information Act, no. 4 of 2013; Children's Act no. 38 of 2005 and the National Health Act, no. 61 of 2003.
6. Only de-identified research data may be used for secondary research purposes in future on condition that the research objectives are similar to those of the original research. Secondary use of identifiable human research data requires additional ethics clearance.
7. No field work activities may continue after the expiry date of **20 November 2023**. Submission of a completed research ethics progress report will constitute an application for renewal of Ethics Research Committee approval.

Note:

*The reference number **2018-DIS-0006** should be clearly indicated on all forms of communication with the intended research participants, as well as the Committee.*

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

Yours sincerely

Dr Isabel Schellnack-Kelly
Department of Information Science: Ethics Committee

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

APPENDIX C: INFORMED CONSENT

CONSENT TO PARTICIPATE IN THE INTERVIEW

Ethics clearance reference number: Rec-221118

ENTRUSTING RECORDS TO THE CLOUD TO SUPPORT E-GOVERNMENT SERVICES IN SOUTH AFRICA

Dear Prospective Participant

My name is Amos Shibambu and I am doing research with Mpho Ngoepe, a professor, in the Department of Information Sciences towards a Doctor of Literature AND Philosophy at the University of South Africa. You are invited to participate in a study entitled entrusting records to the cloud to support e-government services in South Africa

WHAT IS THE PURPOSE OF THE STUDY?

The purpose of this study is to explore entrusting of records to the cloud to support e-government services in South Africa

WHY AM I BEING INVITED TO PARTICIPATE?

You were selected as a possible participant in this study because you are regarded as one of the drivers that play a critical role in ICT and records management. Fellow colleagues within Research and Development section within your organisation referred us to you. We will be interviewing approximately 21 participants coming from the parliament, ICT and records management divisions across various state institutions

WHAT IS THE NATURE OF MY PARTICIPATION IN THIS STUDY?

This is a semi-structured interview where open-ended questions are asked to you to try and answer our research questions. Your expertise as the targeted participant in this study will help answer research questions for this study. Given the nature of a study, I would like to request to

record the interview so that i can use it for reference while proceeding with this study. I will not record this interview without your permission. You have a right to revoke recording permission and/or end the interview at any time. The interview will take around 45 minutes of your time. I may come back for a follow-up interview within three months if the exercise is not complete.

CAN I WITHDRAW FROM THIS STUDY EVEN AFTER HAVING AGREED TO PARTICIPATE?

Your participation in this study is voluntary and you are under no obligation to consent to participation. If you decide to take part, you will be given this information sheet to keep and be asked to sign a written consent form. You are free to withdraw at any time and without giving a reason.

WHAT ARE THE POTENTIAL BENEFITS OF TAKING PART IN THIS STUDY?

Given the knowledge you possess in ICT, records management and law-making in this area, your participation will benefit a great deal in acquiring the knowledge from you. Again, you will have your wealth of knowledge shared in a way that other people were not aware of.

ARE THERE ANY NEGATIVE CONSEQUENCES FOR ME IF I PARTICIPATE IN THE RESEARCH PROJECT?

There is no potential harm or discomfort foreseen for participating in this study. The researchers will ensure that no potential harm may occur to the study participants.

WILL THE INFORMATION THAT I CONVEY TO THE RESEARCHER AND MY IDENTITY BE KEPT CONFIDENTIAL?

You have the right to resist and insist that your name is not recorded anywhere and that no one, apart from the researcher and identified members of the research team, will know about your involvement in this research. Your answers will be given a code number or a pseudonym and you will be referred to in this way in the data, any publications, or other research reporting methods such as conference proceedings.

Your answers may be reviewed by people responsible for making sure that research is done properly, including the transcriber, external coder, and members of the Research Ethics Review Committee. Otherwise, records that identify you will be available only to people working on the study, unless you give permission for other people to see the records.

A report of the study may be submitted for publication, but individual participants will not be identifiable in such a report.

HOW WILL THE RESEARCHER(S) PROTECT THE SECURITY OF DATA?

Hard copies of your answers will be stored by the researcher for a minimum period of five years in a locked cupboard/filing cabinet in a secured place so that future scholars can access it for research purposes. Any digitized information will be stored on a password-protected computer that is encrypted. Future use of the stored data will be subject to further Research Ethics Review and approval if applicable. Any information on the hard copies will be shredded and digital information will be deleted using relevant software.

WILL I RECEIVE PAYMENT OR ANY INCENTIVES FOR PARTICIPATING IN THIS STUDY?

There is no monetary compensation that will be awarded to all participants.

HAS THE STUDY RECEIVED ETHICS APPROVAL?

This study has received written approval from the Research Ethics Review Committee of the Unisa. A copy of the approval letter can be obtained from the researcher if you so wish.

HOW WILL I BE INFORMED OF THE FINDINGS/RESULTS OF THE RESEARCH?

If you would like to be informed of the final research findings, please contact Amos Shibambu on Shibambu.a@dhet.gov.za or Shibambu.a@gmail.com or 0825951275.

Should you require any further information or want to contact the researcher about any aspect of this study, please contact Amos Shibambu on Shibambu.a@dhet.gov.za or Shibambu.a@gmail.com or 0825951275.

Should you have concerns about the way in which the research has been conducted, you may contact Prof Mpho Ngoepe on 0124296360 or via email at ngoepms@unisa.ac.za.

Thank you for taking time to read this information sheet and for participating in this study. Thank you.

Amos Shibambu

CONSENT TO PARTICIPATE IN THIS STUDY

I, _____confirm that the person asking my consent to take part in this research has told me about the nature, procedure, potential benefits and anticipated inconvenience of participation.

I have read (or had explained to me) and understood the study as explained in the information sheet.

I have had sufficient opportunity to ask questions and am prepared to participate in the study.

I understand that my participation is voluntary and that I am free to withdraw at any time without penalty (if applicable).

I am aware that the findings of this study will be processed into a research report, journal publications and/or conference proceedings, but that my participation will be kept confidential unless otherwise specified.

I agree to the recording of the data collection method in the form of interviews.

I have received a signed copy of the informed consent agreement.

Participant Name & Surname…… (Please print)

Participant Signature……..Date……

Researcher's Name & Surname:

Researcher's
signature……Date……